MC

#2 04C0 04-10-

0500

500.39847X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): CH. OKAMOTO, ET AL

Serial No.: 09 / 801,748

Filed: MARCH 9, 2001

Title: "IDENTIFICATION CODE MANAGEMENT METHOD AND MANAGEMENT SYSTEM".

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

MARCH 29, 2001

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on:

Japanese Patent Application No. 2000 - 210689
Filed: JULY 6, 2000

A certified copy of said Japanese Patent Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No. 29,621

CIB/rp
Attachment

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　７月　６日

出願番号
Application Number: 特願２０００－２１０６８９

出願人
Applicant (s): 株式会社日立製作所

２００１年　３月１６日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３０２００８９

【書類名】　特許願
【整理番号】　K00009671
【提出日】　平成12年 7月 6日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 19/00
【請求項の数】　42
【発明者】
【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
【氏名】　岡本　周之
【発明者】
【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
【氏名】　宝木　和夫
【発明者】
【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
【氏名】　福澤　寧子
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社日立製作所
【代理人】
【識別番号】　100075096
【弁理士】
【氏名又は名称】　作田　康夫
【手数料の表示】
【予納台帳番号】　013088
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ＩＤの管理方法及び管理システム

【特許請求の範囲】

【請求項１】

ID発行の受注を行なうID受注端末と、前記IDが格納されたIDタグの製造を行なう製造工場用端末と、ネットワークを介して前記ID受注端末および製造工場用端末に接続されたID管理端末とを含むID管理システムを用いて、IDの管理を行うID管理方法であって、

前記IDタグには、外部からデータを読取り可能な電子回路チップが装着されており、

前記電子回路チップは、書き換え不可の記憶領域を有し、且つ当該領域に、外部から読取り可能なデータとして、受注したIDと、IDの属性情報と、改竄検知符号、とを含む、拡張IDを格納しており、

前記ID管理端末において、

前記ID受注端末から、前記拡張IDを含む受注ID登録要求が送られてきた場合に、当該拡張IDが登録済みであるとして、データベースに登録する受注ID登録ステップと、

前記製造工場用端末から、製造済みの前記IDタグに格納されている前記拡張IDを含む、製造済みID登録要求が送られてきた場合に、当該拡張IDを格納した前記IDタグが製造済みであるとして、前記データベースに登録する製造済みID登録ステップと、を有するID管理方法。

【請求項２】

請求項１記載のID管理方法であって、

前記ID管理端末において、

前記ID受注端末から、前記拡張IDを含むID重複確認要求が送られてきた場合に、当該拡張IDが受注済みであるとして前記データベースに登録されているか否かを調べ、

その結果を前記ID受注端末に通知するID重複確認ステップをさらに有するID管理方法。

【請求項３】

請求項１記載のID管理方法であって、

前記ID管理端末において、

前記IDタグ製造工場用端末から、前記IDタグに格納されている前記拡張IDを含む、欠番ID登録要求が送られてきた場合に、当該要求に含まれる拡張IDが欠番IDであるとして、前記データベースに登録する欠番ID登録ステップをさらに有するID管理方法。

【請求項４】

請求項１記載のID管理方法であって、

前記ID管理システムは、

ネットワークを介して前記ID管理端末に接続された、ID利用端末を含んでおり、

前記ID管理端末において、

前記ID利用端末から、前記拡張IDを含む検証要求が送られてきた場合に、当該拡張IDを、データベースに格納してある拡張IDと比較し、送られてきた拡張IDに含まれる前記改竄検知符号が正当か否かを検証する検証ステップをさらに有するID管理方法。

【請求項５】

請求項１記載のID管理方法であって、

前記ID管理システムは、

ネットワークを介して前記ID管理端末に接続された、ID利用端末を含んでおり、

前記ID管理端末において、

前記ID利用端末から、前記IDの属性情報を含む検証用鍵要求が送られてきた場合に、当該属性情報と対応づけられてデータベースに格納してある、前記改竄検知符号の検証用の鍵を、前記ID利用端末に送信するステップをさらに有するID管理方法。

【請求項６】

請求項１記載のID管理方法であって、

前記ID管理システムは、

ネットワークを介して前記ID管理端末に接続された、ID利用端末を含んでおり、

前記ID管理端末において、

前記ID利用端末から、復号化用鍵要求が送られてきた場合に、データベースに格納してある、暗号化された拡張IDの復号化用の鍵を、前記ID利用端末に送信するステップをさらに有するID管理方法。

【請求項７】

請求項１記載のID管理方法であって、

前記ID管理システムは、

ネットワーク２を介して前記ID管理端末に接続された、ID利用端末を含んでおり、

前記ID管理端末において、

前記ID利用端末から、前記拡張IDを含む、失効ID登録要求が送られてきた場合に、当該要求に含まれる拡張IDが失効IDであるとして、前記データベースに登録する失効ID登録ステップをさらに有するID管理方法。

【請求項８】

請求項１記載のID管理方法であって、

前記ID管理システムは、

ネットワークを介して前記ID受注端末に接続された、顧客端末を含んでおり、

前記ID受注端末において、

前記顧客端末から、前記ＩＤタグを発注する顧客の情報と、前記ＩＤタグへの格納を希望するＩＤと、前記ＩＤの改竄検知符号を生成するための鍵と、を含む発注情報が送られてきた場合に、当該発注情報を用いて、前記IDの属性情報と、前記改竄検知符号と、を生成し、前記拡張IDを生成する拡張ID生成ステップと、

前記顧客端末からの要求に応じて、前記発注情報と、前記拡張IDと、を含む受注情報を送信するステップと、

前記受注情報を含む受注ID登録要求をID管理端末に送信する受注ID登録要求ステップと、

前記拡張IDを含むIDタグ製造要求を前記IDタグ製造工場用端末に送信するIDタグ製造要求ステップと、を有するID管理方法。

【請求項９】

請求項１記載のID管理方法であって、

前記IDタグ製造工場用端末において、

前記ID受注端末から、前記拡張IDを含むIDタグ製造要求が送られてきた場合に、前記IDタグを製造させるステップと、

製造された前記IDタグを検査させるステップと，

前記検査ステップの結果が合格の場合に、前記IDタグに格納されている前記拡張IDを含む、製造済みID登録要求を前記ID管理端末に送信する製造済みID登録要求ステップと、を有するID管理方法。

【請求項１０】

請求項１記載のID管理方法であって、

前記ID利用端末において、

処理動作の指示を受け入れる指示入力ステップと、

前記IDタグに装着されている前記電子回路チップから前記拡張IDを取得するID読み取りステップと、

前記読み取りステップで取得した前記拡張IDの正当性を、当該拡張IDに含まれる前記改竄検知符号を用いて検証する検証ステップと、

前記指示入力ステップで受け入れた指示が情報読取指示である場合に、前記ID読み取りステップで取得した前記拡張IDと対応づけられている情報をデータベースから取り出し、当該情報に応じて定められた処理を行なうステップと、

前記指示入力ステップで受け入れた指示が更新指示である場合に、更新情報を入手し、当該更新情報で、前記ID読み取りステップで取得した前記拡張IDと対応づけられている情報を更新するステップと、

前記指示入力ステップで受け入れた指示が新規登録指示である場合に、新規情報を入手し、当該新規情報を、前記ID読み取りステップで取得した前記拡張IDと対応づけてデータベースに格納するステップと、

前記指示入力ステップで受け入れた指示が失効ＩＤ登録指示である場合に、前

記ＩＤタグの情報と対応づけられている前記拡張ＩＤをデータベースから取り出し、当該拡張IDを含む失効ID登録要求をID管理端末に送信する失効ID登録要求ステップと、

を有するID管理方法。

【請求項１１】

ID発行の受注を行なうID受注端末と、前記IDが格納されたIDタグの製造を行なう製造工場用端末と、ネットワークを介して前記ID受注端末および製造工場用端末に接続されたID管理端末とを含むID管理システムであって、

前記IDタグは、外部からデータを読取り可能な電子回路チップを備え、

前記電子回路チップは、書き換え不可の記憶領域を有し、且つ当該領域に、外部から読取り可能なデータとして、受注したIDと、IDの属性情報と、改竄検知符号、とを含む、拡張IDを格納しており、

前記ID受注端末は、受注時に受け入れた発注情報から生成した受注情報を含む受注ID登録要求を、前記ID管理端末に送る受注ID登録要求処理部を備え、

前記ID管理端末は、前記受注ID登録要求が送られてきた場合に、当該拡張IDが登録済みであるとして、データベースに登録する受注ID登録処理部を備え、

前記製造工場用端末は、製造済みの前記IDタグに格納されている前記拡張IDを含む、製造済みID登録要求を、前記ID管理端末に送らせる製造済みID登録要求処理部を備え、

前記ID管理端末は、前記製造済みID登録要求が送られてきた場合に、当該拡張IDを格納した前記IDタグが製造済みであるとして、前記データベースに登録する製造済みID登録処理部を備えるID管理システム。

【請求項１２】

請求項１１記載のID管理システムであって、

前記ID管理端末において、

前記ID受注端末から、前記拡張IDを含むID重複確認要求が送られてきた場合に、当該拡張IDが受注済みであるとして前記データベースに登録されているか否かを調べ、

その結果を前記ID受注端末に通知するID重複確認処理部をさらに有するID管理シ

ステム。

【請求項１３】

請求項１１記載のID管理システムであって、

前記ID管理端末において、

前記IDタグ製造工場用端末から、前記IDタグに格納されている前記拡張IDを含む、欠番ID登録要求が送られてきた場合に、当該要求に含まれる拡張IDが欠番IDであるとして、前記データベースに登録する欠番ID登録処理部をさらに有するID管理システム。

【請求項１４】

請求項１１記載のID管理システムであって、

前記ID管理システムは、

ネットワークを介して前記ID管理端末に接続された、ID利用端末を含んでおり、

前記ID管理端末において、

前記ID利用端末から、前記拡張IDを含む検証要求が送られてきた場合に、当該拡張IDを、データベースに格納してある拡張IDと比較し、送られてきた拡張IDに含まれる前記改竄検知符号が正当か否かを検証する検証処理部をさらに有するID管理システム。

【請求項１５】

請求項１１記載のID管理システムであって、

前記ID管理システムは、

ネットワークを介して前記ID管理端末に接続された、ID利用端末を含んでおり、

前記ID管理端末において、

前記ID利用端末から、前記IDの属性情報を含む検証用鍵要求が送られてきた場合に、当該属性情報と対応づけられてデータベースに格納してある、前記改竄検知符号の検証用の鍵を、前記ID利用端末に送信する処理部をさらに有するID管理システム。

【請求項１６】

請求項１１記載のID管理システムであって、

前記ID管理システムは、

ネットワークを介して前記ID管理端末に接続された、ID利用端末を含んでおり、

前記ID管理端末において、

前記ID利用端末から、復号化用鍵要求が送られてきた場合に、データベースに格納してある、暗号化された拡張IDの復号化用の鍵を、前記ID利用端末に送信する処理部をさらに有するID管理システム。

【請求項１７】

請求項１１記載のID管理システムであって、

前記ID管理システムは、

ネットワーク２を介して前記ID管理端末に接続された、ID利用端末を含んでおり、

前記ID管理端末において、

前記ID利用端末から、前記拡張IDを含む、失効ID登録要求が送られてきた場合に、当該要求に含まれる拡張IDが失効IDであるとして、前記データベースに登録する失効ID登録処理部をさらに有するID管理システム。

【請求項１８】

請求項１１記載のID管理システムであって、

前記ID管理システムは、

ネットワークを介して前記ID受注端末に接続された、顧客端末を含んでおり、

前記ID受注端末において、

前記顧客端末から、前記ＩＤタグを発注する顧客の情報と、前記ＩＤタグへの格納を希望するＩＤと、前記ＩＤの改竄検知符号を生成するための鍵と、を含む発注情報が送られてきた場合に、当該発注情報を用いて、前記IDの属性情報と、前記改竄検知符号と、を生成し、前記拡張IDを生成する拡張ID生成処理部と、

前記顧客端末からの要求に応じて、前記発注情報と、前記拡張IDと、を含む受注情報を送信する受注情報送信処理部と、

前記受注情報を含む受注ID登録要求をID管理端末に送信する受注ID登録要求処理部と、

前記拡張IDを含むIDタグ製造要求を前記IDタグ製造工場用端末に送信するIDタグ製造要求処理部と、を有するID管理システム。

【請求項１９】

請求項１１記載のID管理システムであって、

前記IDタグ製造工場用端末は、

前記ID受注端末から、前記拡張IDを含むIDタグ製造要求が送られてきた場合に、前記IDタグの製造と、

製造された前記IDタグの検査を指示する制御部と、

前記検査処理部の結果が合格の場合に、前記IDタグに格納されている前記拡張IDを含む、製造済みID登録要求を前記ID管理端末に送信する製造済みID登録要求処理部と、を有するID管理システム。

【請求項２０】

請求項１１記載のID管理システムであって、

前記ID利用端末において、

処理動作の指示を受け入れる指示入力処理部と、

前記IDタグに装着されている前記電子回路チップから前記拡張IDを取得するID読み取り処理部と、

前記読み取り処理部で取得した前記拡張IDの正当性を、当該拡張IDに含まれる前記改竄検知符号を用いて検証する検証処理部と、

前記指示入力処理部で受け入れた指示が情報読取指示である場合に、前記ID読み取り処理部で取得した前記拡張IDと対応づけられている情報をデータベースから取り出し、当該情報に応じて定められた処理を行なう処理部と、

前記指示入力処理部で受け入れた指示が更新指示である場合に、更新情報を入手し、当該更新情報で、前記ID読み取り処理部で取得した前記拡張IDと対応づけられている情報を更新する処理部と、

前記指示入力処理部で受け入れた指示が新規登録指示である場合に、新規情報を入手し、当該新規情報を、前記ID読み取り処理部で取得した前記拡張IDと対応

づけてデータベースに格納する処理部と、

前記指示入力ステップで受け入れた指示が失効ＩＤ登録指示である場合に、前記ＩＤタグの情報と対応づけられている前記拡張ＩＤをデータベースから取り出し、当該拡張IDを含む失効ID登録要求をID管理端末に送信する処理部と、

を有するID管理システム。

【請求項２１】

ネットワークに接続されて用いられ、IDタグに格納された拡張ＩＤの管理を行うID管理端末であって、

前記IDタグは、外部からデータを読取り可能な、書き換え不可の記憶領域を有し、且つ当該領域に、受注したIDと、IDの属性情報と、改竄検知符号、とを含む、拡張IDを格納しており、

前記拡張IDと、当該拡張IDに関連する情報と、を登録するデータベースを記憶する記憶手段と、

前記ネットワークに接続された他の端末と、通信を行う通信手段と、

前記通信手段により、前記他の端末から、受注時に受け入れた発注情報から生成した受注情報を含む受注ID登録要求が送られてきた場合に、当該拡張IDが登録済みであるとして、データベースに登録する受注ID登録手段と、

前記通信手段により、前記他の端末から、製造済みの前記IDタグに格納されている前記拡張IDを含む、製造済みID登録要求が送られてきた場合に、当該拡張IDを格納した前記IDタグが製造済みであるとして、前記データベースに登録する製造済みID登録手段と、を有するID管理端末。

【請求項２２】

請求項２１記載のID管理端末であって、

前記通信手段により、前記他の端末から、前記拡張IDを含むID重複確認要求が送られてきた場合に、当該拡張IDが受注済みであるとして前記データベースに登録されているか否かを調べるID重複確認手段をさらに有し、

前記通信手段は、

前記ID重複確認手段での確認結果を前記他の端末に送信するID管理端末。

【請求項２３】

請求項２１記載のID管理端末であって、

前記通信手段により、前記他の端末から、前記IDタグに格納されている前記拡張IDを含む、欠番ID登録要求が送られてきた場合に、当該拡張IDが欠番IDであるとして、前記データベースに登録する欠番ID登録手段をさらに有するID管理端末。

【請求項２４】

請求項２１記載のID管理端末であって、

前記通信手段により、前記他の端末から、前記拡張IDを含む検証要求が送られてきた場合に、当該拡張IDを、データベースに格納してある拡張IDと比較し、送られてきた拡張IDに含まれる前記改竄検知符号が正当か否かを検証する検証手段をさらに有し、

前記通信手段は、

前記検証手段での検証結果を前記他の端末に送信するID管理端末。

【請求項２５】

請求項２１記載のID管理端末であって、

前記通信手段により、前記他の端末から、前記IDの属性情報を含む検証用鍵要求が送られてきた場合に、当該属性情報と対応づけられてデータベースに格納してある、前記改竄検知符号の検証用の鍵を入手する検証用鍵入手手段をさらに有し、

前記通信手段は、

前記改竄検知符号の検証用の鍵を前記端末に送信するID管理端末。

【請求項２６】

請求項２１記載のID管理端末であって、

前記通信手段により、前記他の端末から、復号化用鍵要求が送られてきた場合に、データベースに格納してある、暗号化された拡張IDの復号化用の鍵を入手する復号化用鍵入手手段をさらに有し、

前記通信手段は、

前記暗号化された拡張IDの復号化用の鍵を前記端末に送信するID管理端末。

【請求項２７】

請求項２１記載のID管理端末であって、

前記通信手段により、前記他の端末から、前記拡張IDを含む失効ID登録要求が送られてきた場合に、当該要求に含まれる拡張IDが失効IDであるとして、前記データベースに登録する失効ID登録手段をさらに有するID管理端末。

【請求項２８】

ネットワークに接続されて用いられ、IDタグに格納されるIDの発行を受注するID受注端末であって、

前記IDタグには、外部からデータを読取り可能な，書き換え不可の記憶領域を有し、且つ当該領域に、受注したIDと、IDの属性情報と、改竄検知符号、とを含む、拡張IDを格納しており、

前記ネットワークに接続された他の端末と，通信を行う通信手段と、

前記他の端末から、前記ＩＤタグを発注する顧客の情報と、前記ＩＤタグへの格納を希望するＩＤと、前記ＩＤの改竄検知符号を生成するための鍵と、を含む発注情報が送られてきた場合に、当該発注情報を用いて、前記IDの属性情報と、前記改竄検知符号と、を生成し、前記拡張IDを生成する拡張ID生成部と、

前記通信手段により、前記発注情報から生成した受注情報を含む受注ID登録要求をID管理端末に送信する受注ID登録要求手段と、

前記通信手段により、前記拡張IDを含むIDタグ製造要求を前記IDタグ製造工場用端末に送信するIDタグ製造要求手段と、を有するID受注端末。

【請求項２９】

請求項２８記載のID受注端末であって、

前記通信手段により、前記拡張IDを含むID重複確認要求を前記他の端末に送信して、前記拡張IDが前記ID管理端末に登録してある拡張IDと重複しているか否かを確認させるID重複確認要求処理部をさらに有するID受注端末。

【請求項３０】

請求項２８記載のID受注端末であって、

乱数を生成し、当該乱数を前記改竄検知符号の生成用の鍵とする手段をさらに有するID受注端末。

【請求項３１】

請求項２８記載のID受注端末であって、

前記拡張IDを暗号化し、暗号化してあることを示す暗号化符号を添付する手段をさらに有するID受注端末。

【請求項３２】

ネットワークに接続されて用いられ、IDタグを製造するIDタグ製造工場で用いるIDタグ製造工場用端末であって、

前記IDタグは、外部からデータを読取り可能な、書き換え不可の記憶領域を有し、且つ当該領域に、受注したIDと、IDの属性情報と、改竄検知符号、とを含む、拡張IDを格納しており、

前記ネットワークに接続された他の端末と、通信を行う通信手段と、

前記通信手段により、前記他の端末から、前記拡張IDを含むIDタグ製造要求が送られてきた場合に、当該製造要求に従った前記IDタグの製造と、製造された前記IDタグの検査を実施させる制御手段と、

前記検査の結果が合格の場合に、前記通信手段により、前記IDタグに格納されている前記拡張IDを含む、製造済みID登録要求を前記他の端末に送信して、当該他の端末に、前記拡張IDを格納したIDタグが製造済みであるとして登録させる製造済みID登録要求手段と、

を有するIDタグ製造工場用端末。

【請求項３３】

請求項３２記載のIDタグ製造工場用端末であって、

前記検査の結果が不合格であり、かつ、前記IDタグの再製造が不要な場合に、前記通信手段により、前記IDタグに格納されている前記拡張IDを含む、欠番ID登録要求を前記他の端末に送信して、当該他の端末に、前記拡張IDが欠番IDであるとして登録させる欠番ID登録要求手段をさらに有するIDタグ製造工場用端末。

【請求項３４】

ネットワークに接続されて用いられ、IDタグを利用する際に用いるID利用端末であって、

前記IDタグには、外部からデータを読取り可能な，書き換え不可の記憶領域を

有し、且つ当該領域に、受注したIDと、IDの属性情報と、改竄検知符号、とを含む、拡張IDを格納しており、

前記拡張IDと、当該拡張IDに関連する情報と、当該拡張IDが格納されている前記IDタグと対応づけられている情報と、を登録するデータベースを記憶する記憶手段と、

前記ネットワークに接続された、前記他の端末と通信を行う通信手段と、

処理動作の指示を受け入れる指示入力手段と、

前記IDタグに装着されている前記電子回路チップから前記拡張IDを取得するID読み取り手段と、

前記読み取り手段で取得した前記拡張IDの正当性を、当該拡張IDに含まれる前記改竄検知符号を用いて検証する検証手段と、

前記指示入力手段で受け入れた指示が情報読取指示である場合に、前記ID読み取り手段で取得した前記拡張IDと対応づけられている情報をデータベースから取り出し、当該情報に応じて定められた処理を行なう手段と、

前記指示入力手段で受け入れた指示が更新指示である場合に、更新情報を入手し、当該更新情報で、前記ID読み取り手段で取得した前記拡張IDと対応づけられている情報を更新する手段と、

前記指示入力手段で受け入れた指示が新規登録指示である場合に、新規情報を入手し、当該新規情報を、前記ID読み取り手段で取得した前記拡張IDと対応づけてデータベースに格納する手段と、

前記指示入力手段で受け入れた指示が失効ＩＤ登録指示である場合に、前記ＩＤタグの情報と対応づけられている前記拡張ＩＤをデータベースから取り出し、当該拡張IDを含む失効ID登録要求をID管理端末に送信する手段と、

を有するID利用端末。

【請求項３５】

請求項３４記載のID利用端末であって、

前記ID読み取り手段で取得した前記拡張IDが暗号化されている場合に、前記記憶手段に格納されている復号化用の鍵を用いて復号化を行なう手段をさらに有するID利用端末。

【請求項３６】

請求項３４記載のID利用端末であって、

前記ID読み取り手段で取得した前記拡張IDが暗号化されており、かつ、前記記憶手段に復号化用の鍵を所有していない場合に、前記通信手段により、復号化用鍵要求を前記他の端末に送信して、当該他の端末に、前記復号化用の鍵を送信させる手段をさらに有するID利用端末。

【請求項３７】

請求項３４記載のID利用端末であって、

前記ID読み取り手段で取得した前記拡張IDに含まれる前記改竄検知符号を検証する鍵を所有していない場合に、前記通信手段により、前記拡張IDを含む検証用鍵鍵要求を前記他の端末に送信して、当該他の端末に、前記検証用鍵を送信させる手段をさらに有するID利用端末。

【請求項３８】

請求項３４記載のID利用端末であって、

前記通信手段により、前記ID読み取り手段で取得した前記拡張IDを含む、検証要求を前記他の端末に送信して、当該他の端末に、前記拡張IDの正当性を検証させる検証要求手段をさらに有し、

前記検証手段は、

検証結果として、前記他の端末から送られてくる前記検証要求に対する結果を用いるID利用端末。

【請求項３９】

ネットワークに接続可能な複数の計算機に、ID発行の受注を行なうID受注端末と、前記IDが格納されたIDタグの製造を行なう製造工場用端末と、ID管理端末とからなるID管理システムを実現させるプログラム製品であって、

前記計算機が読みとり可能な媒体と、

前記ID受注端末となる前記計算機に、受注時に受け入れた発注情報から生成した受注情報を含む受注ID登録要求を、前記ID管理端末に送らせる受注ID登録要求処理部を実現させるモジュールと、

前記ID管理端末となる前記計算機に、前記受注ID登録要求が送られてきた場合

に、当該拡張IDが登録済みであるとして、データベースに登録する受注ID登録処理部を実現させるモジュールと、

前記製造工場用端末となる前記計算機に、製造済みの前記IDタグに格納されている前記拡張IDを含む、製造済みID登録要求を、前記ID管理端末に送らせる製造済みID登録要求処理部を実現させるモジュールと、

前記ID管理端末となる前記計算機に、前記製造済みID登録要求が送られてきた場合に、当該拡張IDを格納した前記IDタグが製造済みであるとして、前記データベースに登録する製造済みID登録処理部を実現させるモジュールと、を備えるプログラム製品。

【請求項４０】

流通を管理するためのIDタグを備える物品であって，

前記IDタグは，前記物品のIDと前記物品に関わる属性情報と，前記IDと前記属性情報に対する改竄検知符号とからなる拡張IDを格納し，

前記IDと、前記属性情報と、前記改竄検知符号と、前記改竄検知符号の検証用の鍵を、関連付けて格納するデータベースを用いて，前記拡張IDの正当性を確認可能としたIDタグを備える物品。

【請求項４１】

請求項４０記載のIDタグを備える物品であって、

前記拡張IDは，さらに，前記IDと前記属性情報との割り当てを制御するクラス情報をさらに含むIDタグを備える物品。

【請求項４２】

請求項４０記載のIDタグを備える物品であって、

前記拡張IDは，さらに，拡張IDの桁数、改竄検知符号の桁数と計算方法を示すバージョン情報を含み，前記改竄検知符号は，前記バージョン情報に対する改竄をも検知するものであるIDタグを備える物品。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、IDの管理を行う技術に関し、特に、改竄検知符号を備えたIDの、発

行と流通の管理を行う技術に関する。

【０００２】

【従来の技術】

従来より、JANコードなどの様々なIDが物品に付与され、物品の管理に利用されている。物品に関する情報を、物品に付与したID(物品識別子)と関連付けて管理することにより、物品を個別に管理することができる。

【０００３】

例えば、コンビニエンスストアなどでは、商品の製造会社や名前や価格を、商品の包装に印字されているJANコードと関連付けて管理しておき、バーコードを読み取ることでJANコードを入力すれば商品の情報を参照できるシステムを利用している。

【０００４】

また、値が正しいものであることを保証するため、IDに誤り検知符号を備える。読み取ったIDの誤り検知符号を所定の計算手順により検証することで、読み取りが正常に行われたか否かが判断できる。さらに、鍵となる数値を利用して計算する誤り検知符号には、鍵を知らない者によるIDの改竄を検知する機能がある。以下では、鍵を利用して計算する誤り検知符号のことを改竄検知符号と呼ぶ。

【０００５】

IDに高い安全性が求められる場合、改竄検知符号を備えたIDを利用する。例えば、身分証明証などのようなIDの付与された物品を人と関連付けることにより、人を個別に管理する場合や、株券や商品券などの有価証券にIDを付与して管理する場合などがある。

【０００６】

【発明が解決しようとする課題】

上記従来のIDの管理方法には、以下のような問題がある。

【０００７】

すなわち、上記コンビニエンスストアの例の様にJANコードを物品のIDとして利用する場合、IDの桁数制限により物品の種類別にIDを振り分けているため、同じ種類の物品において，１つ１つ個別に管理することはできない。また、個別管

理ができるようにJANコードよりも桁数を増やしたIDがあるが、バーコードで表示する場合、スペースの都合により適用できない物品もある。

【０００８】

また、JANコードは誤り検知符号しか備えておらず、鍵を用いた改竄検知符号は備えていない。このため、IDを偽造されるおそれがある。偽造防止のため、IDに改竄検知符号を用いる場合は、安全のため、いくつかのID毎に異なる鍵を利用する必要がある。このため、上記コンビニエンスストアの例の様に、様々な種類のIDを扱う場合、扱うID全ての改竄検知符号の検証用の鍵をあらかじめ用意しておかねばならない。

【０００９】

また、改竄検知符号を備えたIDを利用した物品管理を個人が行なう場合、IDが付与されたシールやテープを入手し、任意の物品に貼り付けて管理する方法などが考えられるが、改竄検知符号の検証用の鍵も管理する必要があり、困難である。

【００１０】

また、IDに高い安全性が求められる場合、IDが重複しないように発行の管理を行なうか、もしくは、同一IDの個数の管理を行なう必要がある。このためには、物品やシールへのIDの印字や、電子タグに利用するメモリへの書き込みも、管理しなければならない。

【００１１】

また、IDが重複しないように安全性高く発行の管理を行なっているものとして、クレジットカードのIDが挙げられる。しかし、クレジットカードのIDのように、サービスや、サービスを受ける人・法人に対して与えられているIDは、物品としての実体がなく情報にすぎないため、発行後に不正に複製されてしまう恐れがある。

【００１２】

本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、改竄検知符号を備え、物品個別に割り当て可能なIDの発行と流通を管理し、IDを利用した物品管理を効率よく、かつ、信頼性高く行うことが可能な仕組みを提供すること

にある。

【００１３】

【課題を解決するための手段】

上記目的を達成するために、本発明では、同じ種類の物品であっても異なるIDを個別に割り当て可能であり，さらに属性情報と改竄検知符号を備えた拡張型物品識別子（以下，拡張IDという）を利用する。属性情報とはIDを分類する情報で、IDの利用分野や、発行を依頼した会社名などを表わす情報である。そして、IDの備える改竄検知符号は、属性情報ごとに異なる鍵を用いて生成する。

【００１４】

また、本発明では、IDの発行と流通を管理するためのID管理端末を設け、ネットワークを介して、IDを利用するためのID利用端末に接続する。ID管理端末には、発行したIDと、IDの属性情報と、改竄検知符号と、改竄検知符号の検証用の鍵を、関連付けて格納する。そして、ID管理端末は、IDとIDの属性情報と改竄検知符号とを含む改竄検知符号１０２の検証要求が、ID利用端末から送られてきた場合、格納しているIDと、それに関連付けられている改竄検知符号とを用いて検証し、結果を端末に返す。以下、検証要求とは、改竄検知符号１０２の検証要求を指す。また、IDの属性情報を含む検証用鍵要求がID利用端末から送られてきた場合、IDの属性情報と関連づけられている検証用の鍵を、端末に返す。ID利用端末は、IDを読み取る機能と、読み取ったIDとIDが付与されている物品の情報とを関連付けて管理する機能と、物品の情報が処理を示すものであった場合にその処理を行なう機能を有している。

【００１５】

また、本発明では、ID受注端末とIDタグ製造工場用端末を設け、ネットワークを介してID管理端末と接続する。ID受注端末は、IDの発行を依頼された日付け、個数、改竄検知符号の生成用の鍵などを格納し、生成用の鍵を用いて改竄検知符号の生成を行なう。IDと、IDの属性情報と、改竄検知符号をひとつにまとめる。暗号通信を利用してID管理端末に送信し、ID管理センタで管理している情報から、発行済みのIDと重複していないことを確認した後、同様に暗号通信を利用してIDタグ製造工場用端末に送信する。ここで、IDがバーコードと同じ情報を示して

いる旨を属性情報に含ませて、複数個の同一IDを発行してもよい。

【００１６】

一方、IDタグ製造工場用端末は、バーコードラベルや電子タグなどのIDタグを製造する製造部に対し、IDと、IDの属性情報と、改竄検知符号を、IDタグ上に印字、もしくは、IDタグ内に格納するよう、指示する。また、IDタグの検査部に対し、完成したIDタグに情報が正しく格納されているかどうかを検査するよう、指示する。そして、製造したIDタグの情報と検査結果を、暗号通信を利用してID管理端末に送信する。

【００１７】

本発明によれば、IDを重複すること無く発行し、物品の個別管理を行なうことが可能となる。また、複数個の同一IDを発行し、IDを既存のバーコードシステムで利用することが可能となる。

【００１８】

また、本発明によれば、IDの利用者は、検証用の鍵や装置を保持していなくても、ID利用端末からID管理端末に、ネットワークを通じてIDタグから読みとった情報（例えば，IDとIDの属性情報と改竄検知符号）を用いた検証要求を送信すれば、検証結果を得ることができる。

【００１９】

また、本発明によれば、IDの利用者は、検証用の鍵を保持していなくても、ID利用端末からID管理端末に、ネットワークを通じてIDの属性情報を含む検証用鍵要求を送信すれば、検証用の鍵を得ることができ、改竄検知符号の検証を行なうことができる。

【００２０】

また、本発明によれば、改竄検知符号の生成用および検証用の鍵や、IDの発行依頼者の情報などの、機密性の高い情報を秘密裏に管理することができる。

【００２１】

また、本発明において、IDタグとして電子回路チップを用いる場合を考える。電子回路チップを製造するには、十分な設備が必要である。そして、電子回路チップを小型・薄型にするほど、電子回路チップを製造できる者が限られてくる。

このため、不正な第三者がIDタグの複製を製造する可能性が低くなる。また、IDを電子回路チップの書き換え不可領域に格納すれば、不正な第三者がIDを改変することはできない。したがって、本発明によれば、ID管理端末が市場に流通するIDタグの個数を管理することができる。

【００２２】

【発明の実施の形態】

以下、本発明の一実施形態が適用されたID管理システムについて説明する。

【００２３】

まず、本実施形態のID管理システムで用いるIDおよびIDタグについて説明する。

【００２４】

図１は本実施形態のID管理システムで用いるIDの一例を示した図である。

【００２５】

図１(a)に示すように、本実施形態で用いるID１００は、IDの属性情報１０１と、改竄検知符号１０２を伴ない、拡張ID２００として一まとめで利用される。属性情報１０１とはID１００を分類する情報で、ID１００の利用分野や、発行を依頼した会社名などを表わす情報である。また、改竄検知符号１０２は、属性情報１０１ごとに異なる鍵を用いて、ID１００と属性情報１０１に対して所定の計算を行ない生成される。改竄検知符号１０２を生成するための計算には、公開鍵暗号、共通鍵暗号、ハッシュ生成関数などを組み合わせたものを利用するとよい。

【００２６】

図１(b)は、図１(a)の３要素にクラス情報１０３が付随する場合を示している。クラス情報とは、ID１００と属性情報１０１の切り分け位置、すなわち、それぞれの桁数を示す情報である。図１(c)、(d)、(e)に示すように、クラス情報１０３を用いれば、拡張ID２００と改竄検知符号１０２が同じ桁数でありながら、ID１００と属性情報１０１の桁数や個数を様々に変えた拡張ID２００を構築することができる。このため、拡張ID２００の受け渡しや、改竄検知符号１０２の生成および検証に用いる仕組みを変えることなく、用途に応じて、ID１００と属性

情報１０１の桁数や個数の組み合わせが最適な拡張ID２００を利用できる。

【００２７】

また、図１(f)は、図１(a)の３要素にバージョン情報１０４が付随する場合を示している。バージョン情報とは、拡張ID２００のバージョンを示す情報である。バージョン情報１０４から、拡張ID２００の桁数、改竄検知符号１０２の桁数と計算方法などが分かる。

【００２８】

また、図１(g)は、拡張ID２００が暗号化してある場合を示している。暗号化してあることを示す暗号化符号１０５と、図１(a)の３要素を暗号化した情報１０６からなる。拡張ID２００を暗号化して用いると、復号化用の鍵を知らない者には拡張ID２００の構成要素が判別できないため、不正な解読を防止することができる。

【００２９】

なお、拡張ID２００は上記に限らず、クラス情報１０３の追加、バージョン情報１０４の追加、暗号化、のうちの任意の２つ、または、全てを組み合わせたものでも良い。

【００３０】

図２は本実施形態のID管理システムで用いるIDタグの一例を示した図である。

【００３１】

図２(a)は、テープ状のIDタグ３００に電子回路チップ３０１が複数個装着されている様子を示す。適切な位置でテープを切断することで、任意の個数の電子回路チップが装着されたテープ片を得ることができる。

【００３２】

なお、IDタグ３００は、電子回路チップ３０１が装着されているテープ状のものとしたが、シート状のものであってもよいし、電子回路チップ３０１そのものでもよい。また、IDが印刷されたラベルであってもよい。

【００３３】

電子回路チップ３０１は、たとえば、十分な設備を有する半導体製造メーカでなければ製造できない0.3mm角程度の小型電子回路チップであり、薄型の略直方

体の形状を有している。また、図２(b)に示すように、シリコンチップ３０２上に、メモリおよびその読み出し回路として機能する電子回路３０３と、コンデンサ３０４と、アンテナ３０５とが、形成されて構成されている。メモリは、書き換え不可能なメモリ部分を含むものとする。また、書き換え不可能なメモリ部分には、拡張ID２００が格納されている。

【００３４】

なお、電子回路３０３の書き換え不可能なメモリ部分への拡張ID２００の格納は、電子回路チップ３０１の製造業者が、当該チップ３０１をIDタグ３００の製造業者へ出荷する前に、予め行っておくようにする。電子回路３０３の書き換え不可能なメモリ部分とは、ROMなどの書き換え不可能なメモリの他、たとえば、拡張ID２００が書き込まれた部分が書き換え不可に設定されている、EEPROMなどの書き換え可能なメモリも含むものとする。

【００３５】

電子回路３０３とコンデンサ３０４とアンテナ３０５は、図２(c)に示すような回路を形成している。この回路は、外部から与えられた電波により、アンテナ３０５にて電流を誘起し、電荷をコンデンサ３０４に蓄積する。そして、コンデンサ３０４に蓄積した電荷から得た電力を用いて、電子回路３０３に記憶されている情報を、アンテナ３０５より電波を用いて送信する。すなわち、この電子回路チップ３０１に電波を与えることにより、外部より非接触で電子回路チップ３０１の電子回路３０３に格納されている拡張ID２００を読み出すことができる。

【００３６】

次に、以上のようなIDタグ３００を利用して拡張ID２００の管理を行う、ID管理システムの構成について説明する。

【００３７】

図３は、本実施形態が適用されたID管理システムの概略図である。

【００３８】

図示するように、本実施形態のID管理システムは、ID受注端末３と、IDタグ製造工場用端末４と、ID管理端末５とが、専用ネットワークやインターネットなどのネットワーク１に接続されて構成される。なお、図３に示す例では、端末３お

よび４をそれぞれ１つ示しているが、複数であってもかまわない。また、顧客端末８は、専用ネットワークやインターネットなどのネットワーク７を介して、ID受注端末３に接続されている。また、ID管理端末５は、専用ネットワークやインターネットなどのネットワーク２を介して、ID利用端末６に接続されている。ネットワーク１とネットワーク２とネットワーク７とは、同じネットワークであってもよい。

【００３９】

顧客端末８は、IDタグ３００を発注するために必要な発注情報を、顧客が入力する端末であり、発注情報をID受注端末３に送信する。

【００４０】

ID受注端末３は、拡張ID２００の発行を受注するための端末であり、顧客端末８から送られてきた発注情報から、ID１００、属性情報１０１、改竄検知符号１０２などを含む拡張ID２００を生成し、IDタグ製造工場用端末４に送信する。

【００４１】

また、IDタグ製造工場用端末４は、IDタグ３００の製造を管理する端末であり、ID受注端末３から送られてきた拡張ID２００が付与されたIDタグ３００の製造状況をID管理端末５に送信する。

【００４２】

また、ID管理端末５は、ID受注端末３とIDタグ製造工場用端末４から送られてくる情報を管理し、ID利用端末６から送られてくる要求に応える。

【００４３】

また、ID利用端末６は、IDタグ３００から拡張ID２００を読み取り、拡張ID２００と関連付けて管理している情報を利用するための端末であり、必要に応じて、ID管理端末５に要求を送信する。

【００４４】

なお、ID管理端末５に、ID受注端末３としての機能を持たせるようにすることで、ID受注端末３を省略してもよい。また、ID管理端末５に、IDタグ製造工場用端末４としての機能を持たせるようにすることで、IDタグ製造工場用端末４を省略してもよい。また、ID管理端末５に、ID利用端末６としての機能を持たせるよ

うにすることで、ID利用端末６を省略してもよい。また、ID受注端末３に、顧客端末８としての機能を持たせるようにすることで、顧客端末８を省略してもよい。

【００４５】

なお、顧客端末８とID利用端末６は複数個あってもよい。

【００４６】

なお、顧客端末８とID受注端末３間、および、ID受注端末３とIDタグ製造工場用端末４間、および、ID受注端末３とID管理端末５間、および、IDタグ製造工場用端末４とID管理端末５間、および、ID管理端末５とID利用端末６間の通信には、暗号を用いることが望ましいが、暗号通信の方式は、それぞれ２つの端末間で通信できれば，異なる方式であってもよい。また、暗号通信を行なう代わりに、あらかじめ認証を行なった後で通信を行なってもよい。

【００４７】

次に、上記のID管理システムを構成する各装置について説明する。

【００４８】

図１６は、顧客端末８の機能構成を示す概略図である。

【００４９】

図示するように、顧客端末８は、入出力部８１と、通信部８２を有する。

【００５０】

入出力部８１は、IDタグ３００の発注に必要な発注情報を受け入れる。発注情報とは、IDタグ３００に格納したいID１００、暗号化した拡張ID２００の復号化用の鍵、など拡張ID２００の生成と管理に必要な情報と、発注者情報、発注日時、納入期限、納入方法指定、などIDタグ３００の発注に必要な情報と、を指す。

【００５１】

また、ID受注端末３から受け取った受注情報を出力する。受注情報とは、前記発注情報と、IDタグ３００に格納される拡張ID２００、ID受注端末３が改竄検知符号を生成するために用いた鍵と、検証するために用いる鍵、自動生成された暗号化用及び復号化用の鍵、など拡張ID２００の管理に必要な情報と、受注日時、納入日時、納入方法、などIDタグ３００の納入に必要な情報と、を指す。

【００５２】

通信部８２は、入出力部８１より受け取った発注情報を含む受注情報要求を、通信用に暗号化し、ネットワーク７を介してID受注端末３に送信する。また、ID受注端末３より、暗号化された受注情報を受け取り、復号化する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。

【００５３】

図４は、ID受注端末３の機能構成を示す概略図である。

【００５４】

図示するように、ID受注端末３は、入出力部３１と、拡張ID生成部３２と、改竄検知符号生成部３３と、通信部３４を有する。

【００５５】

通信部３４は、ネットワーク７を介して顧客端末８より受信した暗号文の復号化を行ない、発注情報を含む受注情報要求を得る。利用する暗号方式は、顧客端末８の通信部８２で利用しているものと同じとする。

【００５６】

入出力部３１は、エラー情報などを出力する。また、発注情報をネットワーク７を介して顧客端末８から受け入れず、直接入力受付する場合に用いる。

【００５７】

拡張ID生成部３２は、通信部３４より受け取った発注情報から、IDの属性情報１０１を生成する。また、改竄検知符号生成部３３に、ID１００と属性情報１０１と改竄検知符号生成用の鍵を渡し、生成された改竄検知符号１０２と検証用の鍵を受け取る。発注情報に改竄検知符号生成用の鍵が含まれていない場合、乱数を生成し、生成した値を改竄検知符号生成用の鍵とする。さらに、ID１００と属性情報１０１と改竄検知符号１０２から、拡張ID２００を生成する。なお、属性情報１０１は、クラス情報１０３であってもよいし、バージョン情報１０４であってもよい。また、発注情報に拡張ID２００の暗号化用の鍵が含まれていない場合、乱数を生成し、生成した値を暗号化用の鍵とする。また、拡張ID２００を暗号化し、暗号化符号１０５を生成し、復号化用の鍵を生成する機能も有する。発

注情報に、拡張ID、生成した鍵などを加え、受注情報とする。

【００５８】

改竄検知符号生成部３３は、拡張ID生成部３２より受け取ったID１００と属性情報１０１と改竄検知符号生成用の鍵から、改竄検知符号１０２と検証用の鍵とを生成し、拡張ID生成部３２に渡す。

【００５９】

通信部３４は、ネットワーク７を介して顧客端末８より受け取った発注情報を含むID重複確認要求を、通信用に暗号化し、ネットワーク１を介してID管理端末５に送信する。なお、発注情報の代わりに入出力部３１より受け取った拡張ID２００を送信してもよい。ID管理端末５より、発行済みIDとの重複がない旨の通知を受け取った後、入出力部３１より受け取った受注情報を含む受注ID登録要求を通信用に暗号化し、ネットワーク１を介してID管理端末５に送信する。なお、IDの重複を許可する場合は、ID重複確認要求の送信を省略しても良い。

【００６０】

また、入出力部３１より受け取った受注情報を含むIDタグ製造要求を通信用に暗号化し、ネットワーク１を介してIDタグ製造工場用端末４に送信する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。また、入出力部３１より受け取った受注情報を通信用に暗号化し、ネットワーク７を介して顧客端末８に送信する。利用する暗号方式は、顧客端末８の通信部８２で利用しているものと同じとする。

【００６１】

図５は、IDタグ製造工場４６の機能構成を示す概略図である。

【００６２】

図示するように、IDタグ製造工場４６は、IDタグ製造工場用端末４と、製造部４２と、検査部４３と、納入部４５とを有する。また、IDタグ製造工場用端末４は、通信部４１と、制御部４４とを有する。

【００６３】

通信部４１は、ネットワーク１を介してID受注端末３より受信した暗号文の復

号化を行ない、受注情報を含むIDタグ製造要求を得る。利用する暗号方式は、ID受注端末３の通信部３４で利用しているものと同じとする。

【００６４】

制御部４４は、通信部４１で得た受注情報を受け取り、該受注情報に含まれる拡張ID２００を格納したIDタグ３００を、該受注情報に従って製造するよう、製造部４２に指示する。また、拡張ID２００を検査部４３に送り、完成したIDタグ３００の機能が正常か否かを検査するよう、検査部４３に指示する。検査結果が不良であった場合、拡張ID２００を製造部４２に渡し、再度、IDタグ３００を製造させる。検査結果が不良であった拡張ID２００を、欠番IDとして通信部４１に渡してもよい。また、検査結果が正常であったIDタグ３００に付与されている拡張ID２００を製造済みIDとして通信部４１に渡す。

【００６５】

通信部４１は、欠番IDを含む欠番ID登録要求と、製造済みIDを含む製造済みID登録要求と、を作成し、通信用に暗号化し、ネットワーク１を介してID管理端末５に送信する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。

【００６６】

製造部４２は、制御部４４より受け取った拡張ID２００を格納したIDタグ３００を製造する。そして、製造したIDタグ３００を検査部４３に渡す。

【００６７】

検査部４３は、製造部４２から受け取ったIDタグ３００を検査し、制御部４４より受け取った拡張ID２００が正しく格納されていることなどを確認する。そして、検査結果を制御部４４に送る。

【００６８】

納入部４５は、検査部４３で検査結果が合格であったIDタグ３００を受け取る。そして、受注情報に含まれる納入方法に従って、顧客に対して発送・引き渡しなどを行ない、納入する。

【００６９】

図６は、ID管理端末５の機能構成を示す概略図である。

【００７０】

図示するように、ID管理端末５は、通信部５１と、ID関連情報管理部５２と、ID関連情報管理データベース５３とを有する。

【００７１】

通信部５１は、ネットワーク１を介してID受注端末３より受信した暗号文の復号化を行ない、受注情報を含むID重複確認要求、もしくは、受注情報を含む受注ID登録要求を得る。利用する暗号方式は、ID受注端末３の通信部３４で利用しているものと同じとする。また、ネットワーク１を介してIDタグ製造工場用端末４より受信した暗号文の復号化を行ない、欠番IDを含む欠番ID登録要求と、製造済みIDを含む製造済みID登録要求と、を得る。利用する暗号方式は、IDタグ製造工場用端末４の通信部４１で利用しているものと同じとする。また、ネットワーク２を介してID利用端末６より受信した暗号文の復号化を行ない、拡張ID２００を含む検証要求、もしくは、属性情報１０１を含む検証用鍵要求、もしくは、復号化用鍵要求を得る。利用する暗号方式は、ID利用端末６の通信部６１で利用しているものと同じとする。

【００７２】

ID関連情報管理部５２は、通信部５１より受け取った要求が、ID重複確認要求である場合、共に受け取った受注情報に含まれる拡張ID２００と、ID関連情報管理データベース５３に格納してある拡張ID２００とを用いて、発行済みIDと重複するか否かを確認する。そして、確認の結果を通信部５１で暗号化し、ネットワーク１を介してID受注端末３に送信する。また、通信部５１より受け取った要求が、受注ID登録要求である場合、共に受け取った受注情報をID関連情報管理データベース５３に格納する。また、通信部５１より受け取った要求が、欠番ID登録要求である場合、共に受け取った欠番IDをID関連情報管理データベース５３に格納する。また、通信部５１より受け取った要求が、製造済みID登録要求である場合、共に受け取った製造済みIDをID関連情報管理データベース５３に格納する。また、通信部５１より受け取った要求が、検証要求である場合、共に受け取った拡張ID２００と、ID関連情報管理データベース５３に格納してある拡張ID２００とを比較し、検証を行なう。そして、検証結果を通信部５１で暗号化し、ネット

ワーク２を介してID利用端末６に送信する。また、通信部５１より受け取った要求が、検証用鍵要求である場合、共に受け取った属性情報１０１から、ID関連情報管理データベース５３に格納してある改竄検知符号１０２の検証用の鍵を取り出し、通信部５１で暗号化し、ネットワーク２を介してID利用端末６に送信する。また、通信部５１より受け取った要求が、復号化用鍵要求である場合、ID関連情報管理データベース５３より復号化用の鍵を取り出し、通信部５１で暗号化し、ネットワーク２を介してID利用端末６に送信する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。また、通信部５１より受け取った要求が、失効ID登録要求である場合、共に受け取った失効ID２００を、ID関連情報管理データベース５３に格納する。

【００７３】

ID関連情報管理データベース５３には、IDタグ３００に関連する管理情報が格納される。図１７は、ID関連情報管理データベース５３に格納されるIDタグ３００に関連する管理情報を説明するための図である。図示するように、IDタグ３００に関連する管理情報は、ID受注端末３から送られてきた受注情報５３０と、発行/納入済み・欠番扱い・製造中・失効などのIDの発行状況５３８と、その他の管理情報である備考５３９と、を含んで構成される。

【００７４】

ここで、受注情報５３０は、顧客端末８において受け入れた発注情報５３１と、ID受注端末３において前記発注情報５３１から生成された拡張ID２００と、を含む。ここで、発注情報５３１は、顧客情報５３２と、顧客が発注したIDの個数５３３と、欠番や重複などの発行条件５３４と、ID３００の指定納入日５３５と、IDの属性情報１０１と対応づけられた改竄検知コード１０２の検証用の鍵５３６と、拡張ID２００が暗号化されてIDタグ３００に付与されている場合の復号化用の鍵５３７と、顧客が発行を希望したID１００と、を含んで構成される。

【００７５】

図７は、ID利用端末６の機能構成を示す概略図である。図示するように、ID利用端末６は、ID読み取り部６１と、入出力部６２と、制御部６３と、データベー

ス６４と、通信部６５とを有する。

【００７６】

ID読み取り部６１は、IDタグ３００に付与された拡張ID２００を読み取る。たとえば、拡張IDが電子回路チップ３０１のメモリに格納されている場合、電波を送信してIDタグ３００に装着された電子回路チップ３０１を駆動する。そして、当該電子回路チップ３０１から送信されるデータを読み取る。受信したデータに暗号化符号１０５がある場合は、受信したデータを復号化し、拡張ID２００を得る。復号化に用いる鍵は、あらかじめデータベース６４に格納しておいてもよいし、通信部６５を通じてID管理端末５に復号化用鍵要求を送信してID管理端末５から入手してもよい。また、読み取った拡張ID２００を含む検証要求を通信部６５を通じてID管理端末５に送信し、ID管理端末５から検証結果を入手してもよい。

【００７７】

入出力部６２は、データベース６４に対し、新規に登録する情報、または、更新する情報の入力、及び、読み出した情報の表示を行なう。また、IDの読み取り、データベースの読み書き、通信、などの指示を受け入れ、結果を出力する。

【００７８】

制御部６３は、ID読み取り部６１と、入出力部６２と、データベース６４と、通信部６５とを制御する。また、読み取った拡張ID２００の改竄検知符号１０２の検証を行なう。検証用の鍵は、データベース６４に格納しておいてもよいし、属性情報１０１を含む検証用鍵要求をID管理端末５に対して送信して、ID管理端末５から入手してもよい。改竄検知符号１０２の検証は、拡張ID２００を含む検証要求をID管理端末５に送信して、検証結果をID管理端末５から入手してもよい。改竄検知符号１０２の検証に成功したならば、対応づけて格納してある情報をデータベース６４から取り出し、入出力部６２で出力する。なお、取り出した情報が処理を示すものである場合、当該処理を行なう。当該処理には、たとえば、決済処理、他の端末への転送、情報が示すURLに対する問い合わせ、などがある。IDの読み取りに失敗した場合は、ID読み取り部６１に再度読み取り作業を行なわせるか、または、当該IDを失効IDとし、電子署名を付加し、通信部６５に失効

ID登録要求をID管理端末５に送信させる。

【００７９】

データベース６４は、拡張ID２００と、拡張ID２００が付与されたIDタグ３００と対応づけられて管理されている物品の情報とを格納する。また、IDの属性情報１０１と、対応する改竄検知符号１０２の検証用の鍵とを、関連付けて格納する。また、IDタグ３００に付与された暗号化した拡張ID２００を復号化するための鍵を格納する。

【００８０】

通信部６５は、復号化用鍵要求と、属性情報１０１を含む検証用鍵要求と、拡張ID２００を含む検証要求と、失効IDを含む失効ID登録要求と、を作成し、通信用に暗号化し、ネットワーク２を介してID管理端末５に送信する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。

【００８１】

なお、ID読み取り部６１と入出力部６２は、ID利用端末６以外の他の端末のものを利用し、ID利用端末６とネットワークを介して接続してもよい。また、ID読み取り部６１と入出力６２は、それぞれ複数個あってもよい。

【００８２】

なお、上記の顧客端末８、ID受注端末３、IDタグ製造工場用端末４、およびID管理端末５は、図８に示すように、CPU７１と、メモリ７２と、ハードディスク装置などの外部記憶装置７３と、FD、CD-ROM、DVD-ROMなどの記憶媒体７４からデータを読み取る記憶媒体読取装置７５と、キーボード、マウスなどの入力装置７６と、モニタなどの出力装置７７と、ネットワークを介して他の装置と通信を行うための通信装置７８と、これら装置間のデータ送受を司るインターフェース７９と、を備えた一般的な構成を有する電子計算機上に、構築することができる。

【００８３】

上記のID受注端末３の入出力部３１、拡張ID生成部３２、改竄検知符号生成部３３、通信部３４、ID管理端末５の通信部５１、ID関連情報管理部５２およびID

関連情報管理データベース５３は、CPU７１がメモリ７２上にロードされたプログラムを実行することで、電子計算機上に具現化されるプロセスとして実現される。また、ID管理端末５の場合、メモリ７２や外部記憶装置７３がID関連情報管理データベース５３として使用される。

【００８４】

この、CPU７１により実行されることで電子計算機上に上記のID受注端末３を具現化するためのプログラムは、予め外部記憶装置７３に記憶され、必要に応じてメモリ７２上にロードされ、CPU７１により実行される。あるいは、記憶媒体読取装置７５を介して記憶媒体７４からメモリ７２上にロードされ、CPU７１により実行される。もしくは、一旦、記憶媒体読取装置７５を介して記憶媒体７４から外部記憶装置７３にインストールされた後、必要に応じて、外部記憶装置７３からメモリ７２上にロードされ、CPU７１により実行される。さらには、他の計算機から、ネットワーク上の伝送媒体と通信装置７８を介して、いったん外部記憶装置７３にダウンロードされ、それからメモリ７２上にロードされ、あるいは直接ネットワークからメモリ７２上にロードされて、CPU７１により実行される。

【００８５】

また、上記のID利用端末６は、図８に示す電子計算機、および、電子回路チップ読取装置、バーコード読取装置、OCR、電子スキャナなどのID読取装置７１０を有するシステム上に、構築することができる。上記のID利用端末６のID読み取り部６１、入出力部６２、制御部６３、データベース６４および通信部６５は、CPU７１がメモリ７２上にロードされたプログラムを実行することで、システム上に具現化されるプロセスとして実現される。また、この場合、メモリ７２や外部記憶装置７３がデータベース６４として使用される。この、CPU７１により実行されることでシステム上に上記のIDタグ製造工場用端末４を具現化するためのプログラムは、予め外部記憶装置７３に記憶され、必要に応じてメモリ７２上にロードされ、CPU７１により実行される。あるいは、記憶媒体読取装置７５を介して記憶媒体７４からメモリ７２上にロードされ、CPU７１により実行される。もしくは、一旦、記憶媒体読取装置７５を介して記憶媒体７４から外部記憶装置

７３にインストールされた後、必要に応じて、外部記憶装置７３からメモリ７２上にロードされ、CPU７１により実行される。さらには、他の計算機から、ネットワーク上の伝送媒体と通信装置７８を介して、いったん外部記憶装置７３にダウンロードされ、それからメモリ７２上にロードされ、あるいは直接ネットワークからメモリ７２上にロードされて、CPU７１により実行される。

【００８６】

次に、上記のID管理システムの動作について説明する。

【００８７】

まず、顧客端末８の動作について説明する。

【００８８】

図１８は、顧客端末８の動作の概略を説明するためのフロー図である。

【００８９】

まず、入出力部８１において、IDタグ３００の発注情報を受け入れる（ステップ１８０１（Ｓ１８０１という，以下同様））。

【００９０】

次に、通信部８２は、Ｓ１８０１で受け入れた発注情報を含む、受注情報要求を作成し、通信用に暗号化してネットワーク７を介してID受注端末３に送信する（Ｓ１８０２）。そして、ID受注端末３から、受注情報を受信するまで待機する（Ｓ１８０３）。受信したならば（Ｓ１８０３のＹｅｓ）、通信部８２は受信した暗号文の復号化を行ない、入出力部８１は、通信部８２で得た受注情報を出力する（Ｓ１８０４）。

【００９１】

次に、ID受注端末３の動作について説明する。

【００９２】

図９は、ID受注端末３の動作の概略を説明するためのフロー図である。

【００９３】

まず、通信部４１は、ネットワーク７を介して顧客端末８から発注情報を含む受注情報要求を受信するまで、待機する（Ｓ１３１６）。受信したならば（Ｓ１３１６のＹｅｓ）、通信部４１は、受信した暗号文の復号化を行ない、発注情報

を入手する（Ｓ１３０１）。

【００９４】

次に、通信部３４は、Ｓ１３０１で受け入れた発注情報を含む、ID重複確認要求を作成し、通信用に暗号化してネットワーク１を介してID管理端末５に送信する（Ｓ１３０２）。そして、ID管理端末５から、前記ID重複確認要求に対する処理結果を受信するまで待機する（Ｓ１３０３）。

【００９５】

次に、発注情報が示すIDとID管理端末５に登録済みのIDとが重複していた場合（Ｓ１３０４のＹｅｓ）、入出力部３１は、エラーを出力する（Ｓ１３０５）。重複していない場合（Ｓ１３０４のＮｏ）、拡張ID生成部３２は、発注情報からIDの属性情報１０１、クラス情報１０３、バージョン情報１０４を生成する（Ｓ１３０６）。発注情報に、改竄検知符号１０２生成用の鍵、または拡張ＩＤ２００の暗号化用の鍵、のいずれかが含まれていない場合（Ｓ１３０７のＮｏ）は、拡張ID生成部３２は、乱数を生成する（Ｓ１３０８）。

【００９６】

次に、改竄検知符号生成部３３は、発注情報に含まれる改竄検知符号１０２生成用の鍵と、ID１００と、Ｓ１３０６で生成された属性情報１０１、クラス情報１０３またはバージョン情報１０４と、を用いて改竄検知符号１０２と、検証用の鍵と、を生成する（Ｓ１３０９）。発注情報に、改竄検知符号１０２生成用の鍵が含まれていない場合は、改竄検知符号１０２生成用の鍵として、Ｓ１３０８で入手した乱数値を用いる。

【００９７】

次に、拡張ID生成部３２は、発注情報に含まれるID１００と、Ｓ１３０６で生成された属性情報１０１、クラス情報１０３またはバージョン情報１０４と、Ｓ１３０９で生成された改竄検知符号１０２と、を用いて拡張ID２００を生成する（Ｓ１３１０）。拡張ID２００の暗号化が必要であった場合（Ｓ１３１１のＹｅｓ）は、拡張ID生成部３２は、発注情報に含まれる暗号化用の鍵を用いて暗号化を行ない（Ｓ１３１２）、暗号化符号１０５を添付する（Ｓ１３１３）。発注情報に、暗号化用の鍵が含まれていない場合は、暗号化用の鍵として、Ｓ１３０８

で入手した乱数値を用いる。

【００９８】

次に、通信部３４は、Ｓ１３０１で受け入れた発注情報と、Ｓ１３１０で作成した拡張ID２００、もしくは、Ｓ１３１３で作成した暗号化した拡張ID２００と、Ｓ１３０８で生成した乱数値から得た鍵と、を含む受注情報を生成する（Ｓ１３１７）。

【００９９】

次に、通信部３４は、Ｓ１３１７で生成した受注情報を含む、受注ID登録要求を作成し、通信用に暗号化してネットワーク１を介してID管理端末５に送信する（Ｓ１３１４）。また、通信部３４は、Ｓ１３１７で生成した受注情報を含む、IDタグ製造要求を作成し、通信用に暗号化してネットワーク１を介してIDタグ製造工場用端末４に送信する（Ｓ１３１５）。また、通信部３４は、Ｓ１３１７で生成した受注情報を、通信用に暗号化してネットワーク７を介して顧客端末８に送信する（Ｓ１３１８）。

【０１００】

なお、Ｓ１３１４、Ｓ１３１５、およびＳ１３１８の順番は入れ替わってもよい。

【０１０１】

なお、Ｓ１３０６～Ｓ１３１０の処理を、Ｓ１３０１の直後に行なってもよい。この場合は、Ｓ１３０２において作成するID重複確認要求には、Ｓ１３１０で生成された拡張ID２００が含まれる。

【０１０２】

次に、IDタグ製造工場用端末４の動作について説明する。

【０１０３】

図１０は、IDタグ製造工場用端末４の動作を説明するためのフロー図である。

【０１０４】

まず、通信部４１は、ネットワーク１を介してID受注端末３からIDタグ製造要求を受信するまで、待機する（Ｓ１４０１）。受信したならば（Ｓ１４０１のＹｅｓ）、通信部４１は、受信した暗号文の復号化を行ない、受注情報を入手する

（Ｓ１４０２）。

【０１０５】

次に、制御部４４は、Ｓ１４０２で入手した受注情報に含まれる拡張ID２００を格納したIDタグ３００を製造するよう、製造部４２に指示し、製造部４２は、該受注情報に従ってIDタグ３００を製造する（Ｓ１４０３）。

【０１０６】

次に、制御部４４は、Ｓ１４０３で製造されたIDタグ３００の機能が正常か否かを検査するよう、検査部４３に指示し、検査部４３は、製造部４２から受け取ったIDタグ３００を検査し、制御部４４より受け取った拡張ID２００が正しく格納されていることなどを確認する。（Ｓ１４０４）。

【０１０７】

制御部４４は、検査部４３から受け取った検査結果が正常であったならば（Ｓ１４０５のＹｅｓ）、IDタグ３００に付与されている拡張ID２００を、製造済みIDとする（Ｓ１４０６）。通信部４１は、Ｓ１４０６で得た製造済みIDを含む、製造済みID登録要求を作成し、通信用に暗号化してネットワーク１を介してID管理端末５に送信する（Ｓ１４０７）。

【０１０８】

次に、納入部４５は、検査部４３で検査結果が合格であったIDタグ３００を受け取り、受注情報に含まれる納入方法に従って、顧客に対して発送・引き渡しなどを行ない、納入する（Ｓ１４１１）。

【０１０９】

一方、検査部４３から受け取った検査結果が異常であったならば（Ｓ１４０５のＮｏ）、制御部４４は、IDタグ３００に付与されている拡張ID２００を、欠番IDとする（Ｓ１４０８）。検査結果が異常であったIDタグ３００の再製造が必要な場合（Ｓ１４０９のＹｅｓ）、制御部４４は、製造部４２にIDタグ３００の再製造を行なわせ、Ｓ１４０８で得た欠番IDを付与する（Ｓ１４０３）。一方、再製造が必要ない場合（Ｓ１４０９のＮｏ）、通信部４１は、欠番IDを含む欠番ID登録要求を作成し、通信用に暗号化してネットワーク１を介してID管理端末５に送信する（Ｓ１４１０）。

【０１１０】

次に、ID管理端末５の動作について説明する。

【０１１１】

図１１は、ID管理端末５の動作を説明するためのフロー図である。

【０１１２】

まず、通信部５１は、ID受注端末３またはIDタグ製造工場用端末４からネットワーク１を介した要求、もしくは、ID利用端末６からネットワーク２を介した要求、を受信するまで、待機する（Ｓ１５０１）。受信したならば（Ｓ１５０１のＹｅｓ）、通信部５１は、受信した暗号文の復号化を行ない、後述する各種情報を含んだ要求を得る（Ｓ１５０２）。

【０１１３】

次に、ID関連情報管理部５２は、Ｓ１５０２で入手した要求内容を解析する。

【０１１４】

入手した要求内容が、ID受注端末３からのID重複確認要求であるならば、ID関連情報管理部５２は、前記ID重複確認要求に含まれる発注情報を入手する（Ｓ１５１１）。次に、Ｓ１５１１で入手した発注情報に含まれる拡張ID２００と、ID関連情報管理データベース５３に格納してある拡張ID２００と、を用いて、IDが重複するか否かを確認する（Ｓ１５１２）。ID関連情報管理データベース５３に同一の拡張ＩＤ２００が格納されていても、該拡張ＩＤ２００が失効扱いであるならば、重複していないものとする。そして、確認の結果を通信部５１で暗号化し、ネットワーク１を介してID受注端末３に送信する（Ｓ１５１３）。

【０１１５】

入手した要求内容が、ID受注端末３からの受注ID登録要求であるならば、ID関連情報管理部５２は、前記受注ID登録要求に含まれる、受注情報を入手する（Ｓ１５２１）。次に、Ｓ１５２１で入手した受注情報を、ID関連情報管理データベース５３に格納する（Ｓ１５２２）。

【０１１６】

入手した要求内容が、IDタグ製造工場用端末４からの製造済みID登録要求であるならば、ID関連情報管理部５２は、前記製造済みID登録要求に含まれる製造済

みIDを入手する（Ｓ１５３１）。次に、Ｓ１５３１で入手した製造済みIDを、ID関連情報管理データベース５３に格納する（Ｓ１５３２）。

【０１１７】

入手した要求内容が、IDタグ製造工場用端末４からの欠番ID登録要求であるならば、ID関連情報管理部５２は、前記欠番ID登録要求に含まれる欠番IDを入手する（Ｓ１５４１）。次に、Ｓ１５４１で入手した欠番IDを、ID関連情報管理データベース５３に格納する（Ｓ１５４２）。

【０１１８】

入手した要求内容が、ID利用端末６からの検証要求であるならば、ID関連情報管理部５２は、検証要求に含まれる拡張ID２００を入手する（Ｓ１５５１）。次に、Ｓ１５５１で入手した拡張ID２００と、ID関連情報管理データベース５３に格納してある拡張ID２００と、を比較して、改竄検知符号１０２が正当なものであるか否かを検証する（Ｓ１５５２）。そして、検証の結果を通信部５１で暗号化し、ネットワーク２を介してID利用端末６に送信する（Ｓ１５５３）。

【０１１９】

入手した要求内容が、ID利用端末６からの検証用鍵要求であるならば、ID関連情報管理部５２は、前記改竄検知符号１０２の検証用鍵要求に含まれる属性情報１０１を入手する（Ｓ１５６１）。次に、Ｓ１５６１で入手した属性情報１０１と関連付けられてID関連情報管理データベース５３に格納してある、改竄検知符号１０２の検証用の鍵を取り出す（Ｓ１５６２）。そして、Ｓ１５６２で取り出した改竄検知符号１０２の検証用の鍵を通信部５１で暗号化し、ネットワーク２を介してID利用端末６に送信する（Ｓ１５６３）。

【０１２０】

入手した要求内容が、ID利用端末６からの復号化用鍵要求であるならば、ID関連情報管理部５２は、ID関連情報管理データベース５３に格納してある、暗号化拡張ID２００の復号化用の鍵を取り出す（Ｓ１５７１）。次に、Ｓ１５７１で取り出した暗号化拡張ID２００の復号化用の鍵を、通信部５１で暗号化し、ネットワーク２を介してID利用端末６に送信する（Ｓ１５７２）。

【０１２１】

入手した要求内容が、ID利用端末６からの失効ID登録要求であるならば、ID関連情報管理部５２は、前記失効ID登録要求に含まれる、失効IDと電子署名を入手する（Ｓ１５８１）。次に、Ｓ１５８１で入手した電子署名により正当な失効ＩＤ登録要求であることを確認し、Ｓ１５８１で入手した失効IDを、ID関連情報管理データベース５３に格納する（Ｓ１５８２）。

【０１２２】

次に、ID利用端末６の動作について説明する。

【０１２３】

図１２は、ID利用端末６の動作の概略を説明するためのフロー図である。

【０１２４】

まず、入出力部６２において、指示入力を受け入れる（Ｓ１６０１）。

【０１２５】

次に、制御部６３は、Ｓ１６０１で受け入れた指示の解析を行なう（Ｓ１６０２）。

【０１２６】

Ｓ１６０１で受け入れた指示が、情報の読み取り指示、または、情報の更新指示、または、情報の新規登録指示の場合、読み取り部６１、制御部６３、データベース６４および通信部６５は、ID読取手続（Ｓ１６０３）を行なう。Ｓ１６０３についての詳細は図１３～１５で説明する。

【０１２７】

Ｓ１６０１で受け入れた指示が、失効登録指示の場合、制御部６３、データベース６４および通信部６５は、読み取ろうとしたIDタグ３００に付与されている拡張ID２００を失効扱いとするための失効手続（Ｓ１６０４）を行なう。Ｓ１６０４についての詳細は図１９で説明する。

【０１２８】

Ｓ１６０１で受け入れた指示が、情報の読み取り指示の場合、Ｓ１６０３の後、制御部６３は、データベース６４より、Ｓ１６０３で入手した拡張ID２００と対応づけられて格納されている情報を取り出す（Ｓ１６０５）。そして、Ｓ１６

０５で取り出した情報を入出力部６２で出力する、情報の指示に従い決済処理を行なう、情報が示す端末へ転送処理を行なう、など、情報に応じた処理を行なう（Ｓ１６０６）。

【０１２９】

Ｓ１６０１で受け入れた指示が、更新情報を含む、情報の更新指示の場合、Ｓ１６０３の後、制御部６３は、更新情報を入手する（Ｓ１６０７）。そして、データベース６４に、Ｓ１６０３で入手した拡張ID２００と対応づけられて格納されている情報を、Ｓ１６０７で入手した更新情報で更新する（Ｓ１６０８）。

【０１３０】

Ｓ１６０１で受け入れた指示が、対応情報を含む、情報の新規登録指示の場合、Ｓ１６０３の後、制御部６３は、対応情報を入手する（Ｓ１６０９）。そして、Ｓ１６０９で入手した対応情報と、Ｓ１６０３で入手した拡張ID２００と、を対応づけて、データベース６４に格納する（Ｓ１６１０）。

【０１３１】

図１３は、図１２に示すＳ１６０３（ID読取手続）の処理の概要を説明するためのフロー図である。

【０１３２】

まず、ID読み取り部６１は、電波を送信してIDタグ３００に装着された電子回路チップ３０１を駆動する。そして、当該電子回路チップ３０１から送信されるデータを読み取る（Ｓ１６１１）。

【０１３３】

次に、制御部６３は、Ｓ１６１１で読み取ったデータに暗号化符号１０５がある場合（Ｓ１６１２のＹｅｓ）、復号化手続を行なう（Ｓ１６１３）。なお、Ｓ１６１３についての詳細は図１４で説明するため、ここでは省略する。

【０１３４】

次に、制御部６３は、Ｓ１６１１で読み取ったデータ、もしくは、Ｓ１６１３で復号化を行なって入手したデータ、の検証手続を行なう（Ｓ１６１４）。なお、Ｓ１６１４についての詳細は図１５で説明するため、ここでは省略する。

【０１３５】

Ｓ１６１４の結果がエラーの場合（Ｓ１６１５のＹｅｓ）、制御部６３は、再読み取りの規定回数内か否かを判断する。（Ｓ１６１８）。規定回数内の場合（Ｓ１６１８のＹｅｓ）は、再度、ＩＤの読み取りを行なう（Ｓ１６１１）。読み取り回数が規定回数に達している場合（Ｓ１６１８のＮｏ）、入出力部６２にエラーを出力する（Ｓ１６１６）。

【０１３６】

一方、Ｓ１６１４の結果がエラーでない場合（Ｓ１６１５のＮｏ）、制御部６３は、正当に検証された拡張ID２００を入手する（Ｓ１６１７）。

【０１３７】

図１４は、図１３に示すＳ１６１３（復号化手続）の処理を説明するためのフロー図である。

【０１３８】

まず、制御部６３は、データベース６４に、復号化用の鍵が格納されているか否かを確認する（Ｓ１６２１）。格納されていない場合（Ｓ１６２１のＮｏ）は、通信部６５は、復号化用鍵要求を作成し、通信用に暗号化してネットワーク２を介してID管理端末５に送信する（Ｓ１６２２）。そして、ID管理端末５から復号化用の鍵を受信するまで待機する（Ｓ１６２３）。

【０１３９】

次に、制御部６３は、データベース６４に格納されている復号化用の鍵、もしくは、Ｓ１６２３で得た復号化用の鍵、を用いて、暗号化拡張ＩＤ２００を復号化する（Ｓ１６２４）。

【０１４０】

図１５は、図１３に示すＳ１６１４（検証手続）の処理を説明するためのフロー図である。

【０１４１】

図１３に示すＳ１６１４（検証手続）の処理の一例として、まず、図１５(a)を説明する。

【０１４２】

まず、制御部６３は、データベース６４に、検証用の鍵が格納されているか否かを確認する（Ｓ１６３１）。格納されていない場合（Ｓ１６３１のＮｏ）は、通信部６５は、属性情報１０１を含む検証用鍵要求を作成し、通信用に暗号化してネットワーク２を介してID管理端末５に送信する（Ｓ１６３２）。そして、ID管理端末５から検証用の鍵を受信するまで待機する（Ｓ１６３３）。

【０１４３】

次に、制御部６３は、データベース６４に格納されている検証用の鍵、もしくは、Ｓ１６３３で得た検証用の鍵、を用いて、改竄検知符号１０２の検証を行なう（Ｓ１６３４）。

【０１４４】

図１３に示すＳ１６１４（検証手続）の処理のもう一つの例として、図１５(b)を説明する。

【０１４５】

通信部６５は、拡張ID２００を含む検証要求を作成し、通信用に暗号化してネットワーク２を介してID管理端末５に送信する（Ｓ１６３５）。そして、ID管理端末５から検証結果を受信するまで待機する（Ｓ１６３６）。

【０１４６】

図１９は、図１２に示すＳ１６０４（失効手続）の処理を説明するためのフロー図である。

【０１４７】

まず、入出力部６２において、読み取りに失敗したＩＤタグ３００に関して、該ＩＤタグ３００の表面に印字されている記号や、該ＩＤタグ３００が付与されていた物品の情報、など、該ＩＤタグ３００に付与されている拡張ＩＤ２００を推定するためのタグ情報の入力を得る（Ｓ１６４１）。

【０１４８】

次に、制御部６３は、Ｓ１６４１で受け入れたタグ情報をデータベース６４で検索し、対応づけられている拡張ＩＤ２００を取り出す（Ｓ１６４２）。取り出した拡張ＩＤ２００を失効ＩＤとする（Ｓ１６４３）。

【０１４９】

次に、通信部６５は、電子署名を生成する（Ｓ１６４４）。該電子署名と失効ＩＤとを含む、失効ＩＤ登録要求を作成し、通信用に暗号化してネットワーク２を介してID管理端末５に送信する（Ｓ１６４５）。

【０１５０】

以上、本発明の一実施形態について説明した。

【０１５１】

本実施形態によれば、ID受注端末３と、ID製造工場用端末４およびID管理端末５は、ネットワーク１を介して暗号通信を行なっている。また、受注情報、発行済みID、欠番IDなどの情報をID管理端末５において一括管理している。また、IDタグ３００として、拡張ID２００が書き換え不可領域に格納された電子回路チップ３０１を利用しているため、不正な第三者が、IDタグ３００に付与されている拡張ID２００を改変することはできない。また、電子回路チップ３０１を製造するには、十分な設備が必要である。そして、電子回路チップ３０１を小型・薄型にするほど、電子回路チップ３０１を製造できる者が限られてくるため、不正な第三者がIDタグの複製を製造する可能性が低くなる。また、ＩＤを失効扱いとする際には、その旨を要求してきたＩＤ利用端末６の電子署名を確認し、正当な権利を有する場合のみ、ＩＤを失効扱いとする。以上のことより、ID管理端末５が市場に流通するIDタグ３００の個数を管理することができる。また、機密性の高い情報を秘密裏に管理することができる。

【０１５２】

また、本実施形態では、ID利用端末６に、検証用の鍵や装置を保持していなくても、ID管理端末５に、ネットワーク２を通じてID１００とIDの属性情報１０１と改竄検知符号１０２とを含む検証要求を送信すれば、検証結果を得ることができる。

【０１５３】

また、本実施形態では、ID利用端末６に、検証用の鍵を保持していなくても、ID管理端末５に、ネットワーク２を通じてIDの属性情報１０１を含む検証用鍵要求を送信すれば、検証用の鍵を得ることができる。

【０１５４】

なお、本発明は、上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【０１５５】

たとえば、上記の実施形態において、ID利用端末６は、必ずしも１つの装置上に構築されているものである必要はない。たとえば、拡張ID２００の読み取りや、情報または指示の入出力に係わる部分と、データベース６４に係わる部分とを、それぞれ別個の装置上に構築し、これらの装置をネットワークで接続するような構成としてもよい。また、それとは逆に、ID利用端末６のデータベース６４に係わる部分の機能をID管理端末５に持たせてもかまわない。

【０１５６】

また、たとえば、上記の実施形態において、顧客端末８からID受注端末３に送られてくる受注情報要求に含まれる発注情報に、検証用鍵または暗号用鍵が含まれていない場合、ID受注端末３で乱数を生成し、該乱数を鍵として扱うことにしているが、乱数生成機能を顧客端末８に持たせてもよい。この場合、顧客端末８において、生成した乱数を検証用鍵または暗号用鍵として発注情報に含ませ、ID受注端末３に送る。

【０１５７】

【発明の効果】

以上説明したように、本発明によれば、改竄検知符号を備えたIDの発行と流通を管理し、IDを利用した物品管理を効率よく、かつ、信頼性高く行うことが可能な仕組みを提供できる。

【図面の簡単な説明】

【図１】

本実施形態のID管理システムで用いるIDの一例を示した図である。

【図２】

本実施形態のID管理システムで用いるIDタグの一例を示した図である。

【図３】

本実施形態が適用されたID管理システムの概略図である。

【図４】

図３に示すID受注端末３の機能構成を示す概略図である。

【図５】

図３に示すIDタグ製造工場４６の機能構成を示す概略図である。

【図６】

図３に示すID管理端末５の機能構成を示す概略図である。

【図７】

図３に示すID利用端末６の機能構成を示す概略図である。

【図８】

図３に示すID管理システムを構成する各装置３～６、および８のハードウエア構成例を示す図である。

【図９】

図４に示すID受注端末３の動作を説明するためのフロー図である。

【図１０】

図５に示すIDタグ製造工場用端末４の動作を説明するためのフロー図である。

【図１１】

図６に示すID管理端末５の動作を説明するためのフロー図である。

【図１２】

図７に示すID利用端末６の動作の概要を説明するためのフロー図である。

【図１３】

図１２に示すＳ１６０２（ID読取手続）の処理の概要を説明するためのフロー図である。

【図１４】

図１３に示すＳ１６１３（復号化手続）の処理を説明するためのフロー図である。

【図１５】

図１３に示すＳ１６１４（検証手続）の処理を説明するためのフロー図である。

【図１６】

図３に示す顧客端末８の機能構成を示す概略図である。

【図１７】

図６に示すＩＤ管理端末５のＩＤ関連情報管理データベース５３に格納されるIDタグ３００に関連する管理情報を説明するための図である。

【図１８】

図１６に示す顧客端末８の動作を説明するためのフロー図である。

【図１９】

図１２に示すＳ１６０４（失効手続）の処理の概要を説明するためのフロー図である。

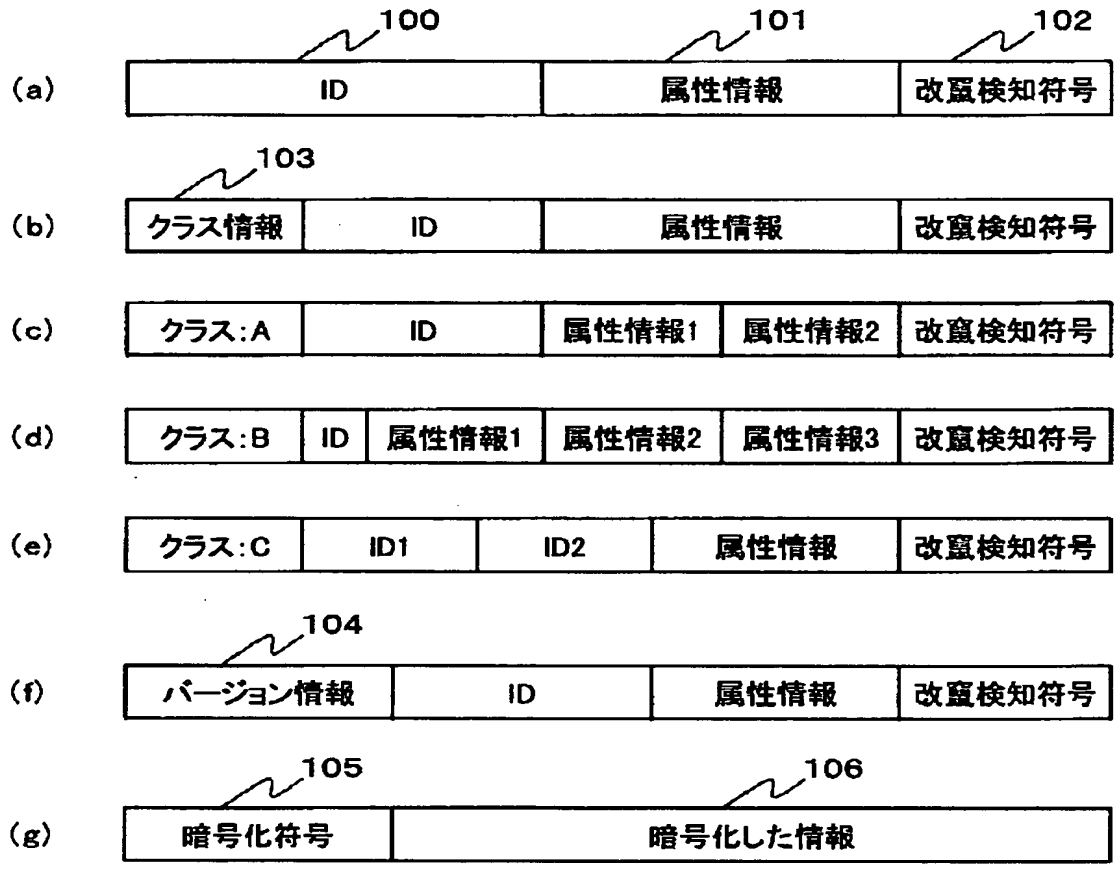
【符号の説明】

１…ネットワーク，３…ID受注端末，４…製造工場用端末，５…ID管理端末，１００…ID，１０１…IDの属性情報，１０２…改竄検知符号，２００…拡張ID，３００…IDタグ，３０１…電子回路チップ。

【書類名】　図面

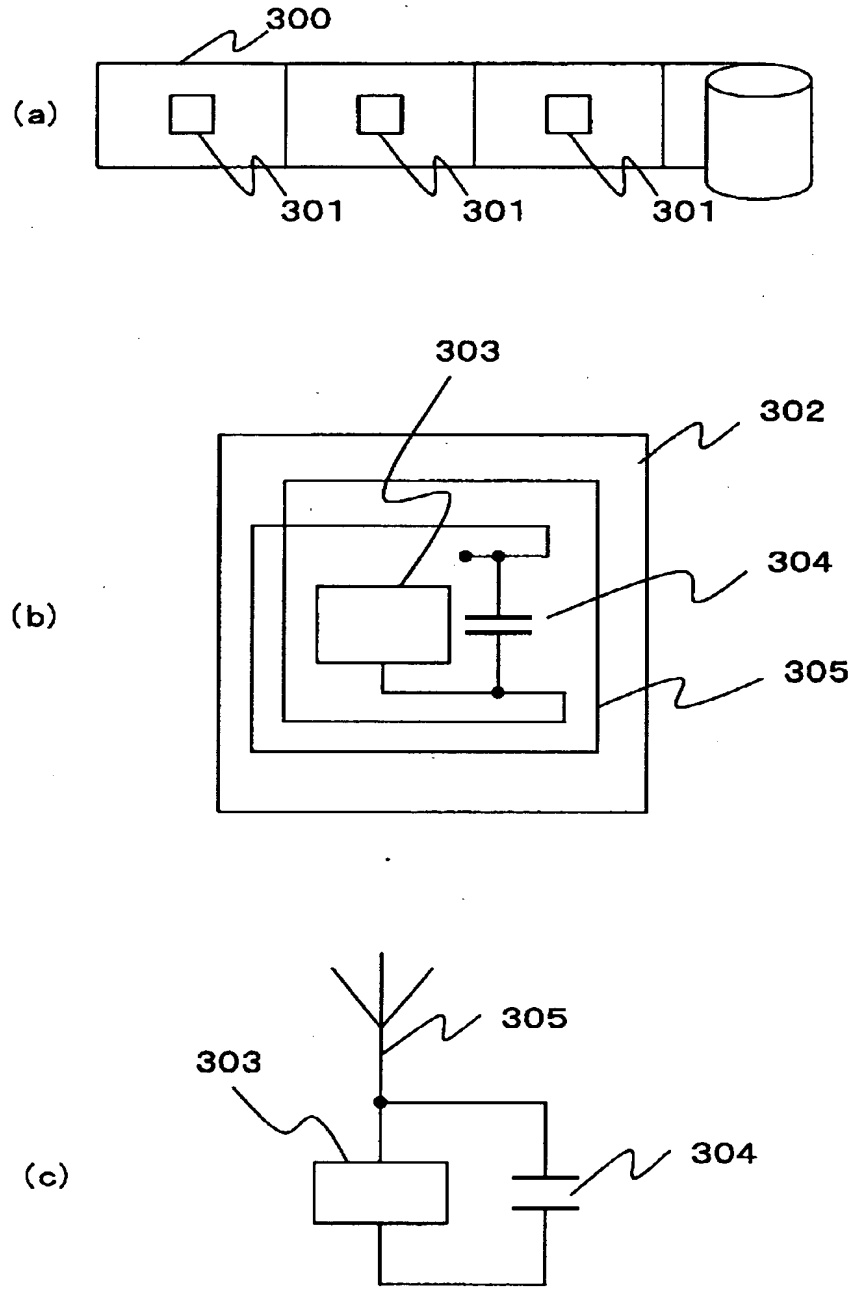
【図１】

図1


100
101
102
(a)
ID
属性情報
改竄検知符号
103
(b)
クラス情報
ID
属性情報
改竄検知符号
(c)
クラス:A
ID
属性情報1
属性情報2
改竄検知符号
(d)
クラス:B
ID
属性情報1
属性情報2
属性情報3
改竄検知符号
(e)
クラス:C
ID1
ID2
属性情報
改竄検知符号
104
(f)
バージョン情報
ID
属性情報
改竄検知符号
105
106
(g)
暗号化符号
暗号化した情報

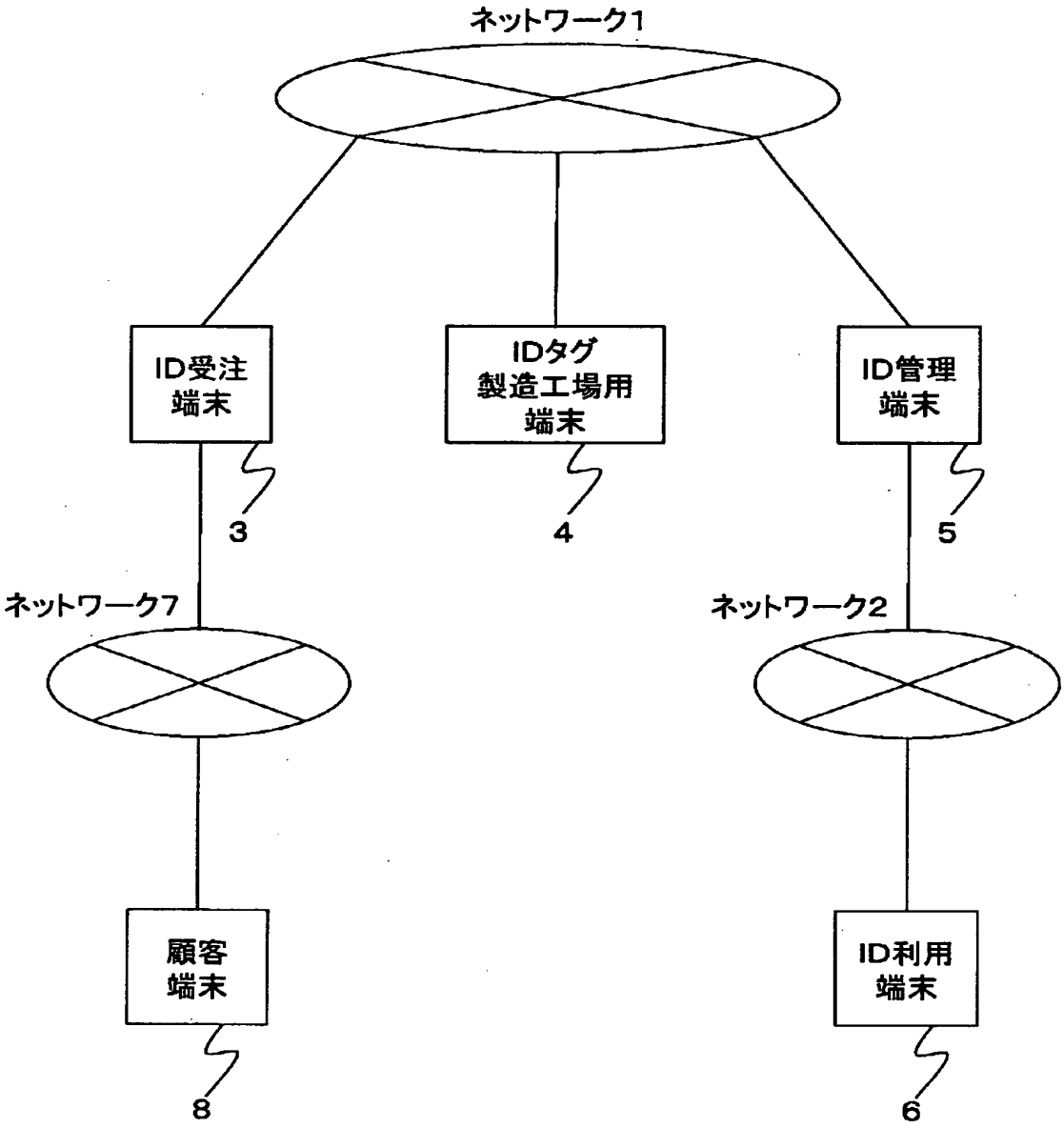
【図２】

図2



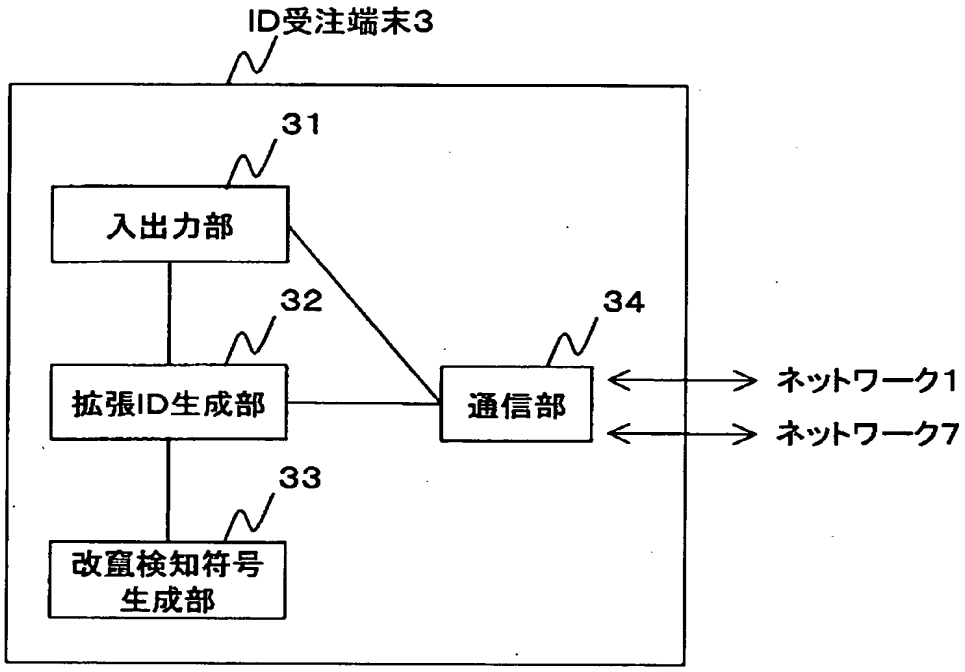
【図３】

図3


ネットワーク1
ID受注
端末
IDタグ
製造工場用
端末
ID管理
端末
3
4
5
ネットワーク7
ネットワーク2
顧客
端末
ID利用
端末
8
6

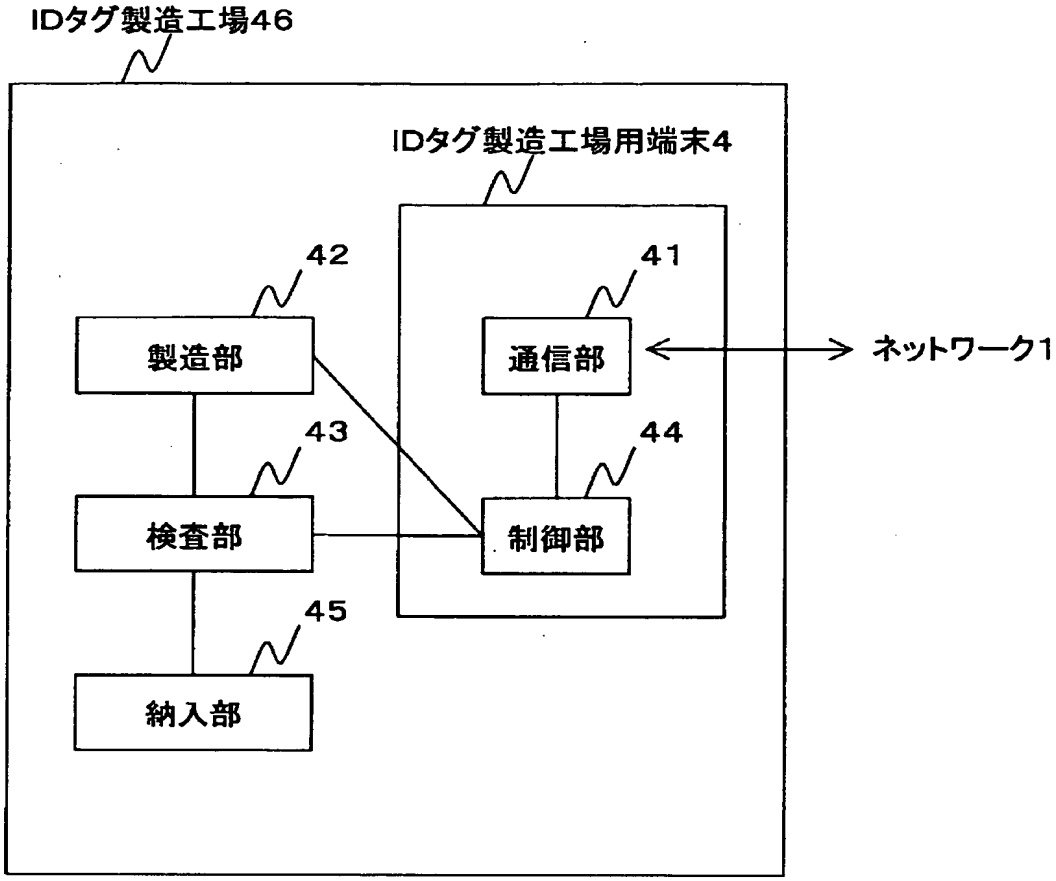
【図４】

図4


ID受注端末3
31
入出力部
32
拡張ID生成部
33
改竄検知符号
生成部
34
通信部
ネットワーク1
ネットワーク7

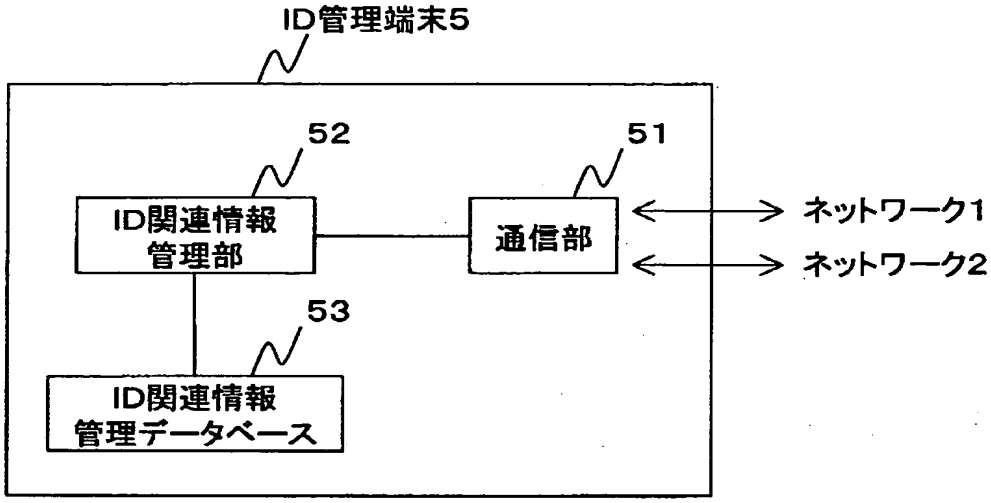
【図５】

図5


IDタグ製造工場46
IDタグ製造工場用端末4
42
41
製造部
通信部
ネットワーク1
43
44
検査部
制御部
45
納入部

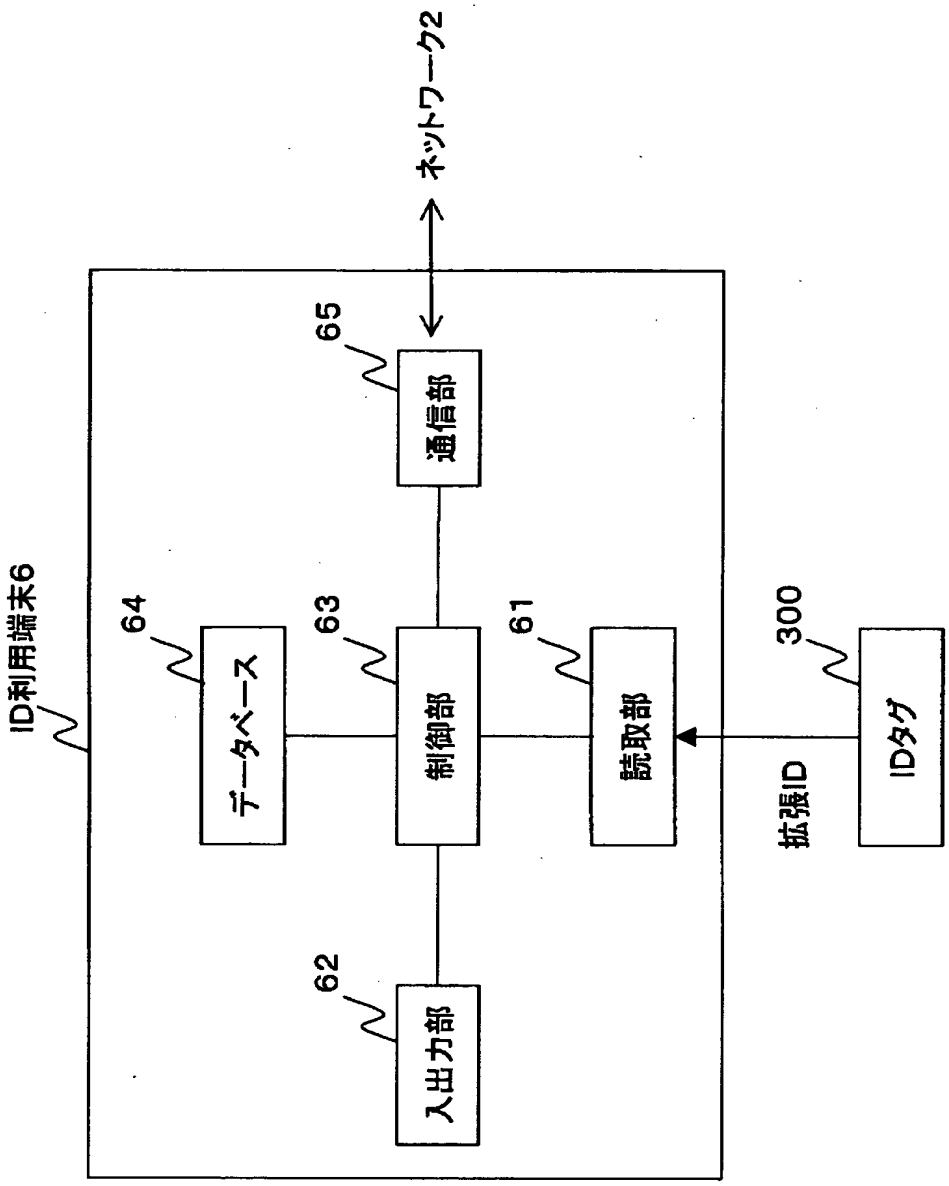
【図６】

図6


ID管理端末5
52
51
ID関連情報
管理部
通信部
ネットワーク1
ネットワーク2
53
ID関連情報
管理データベース

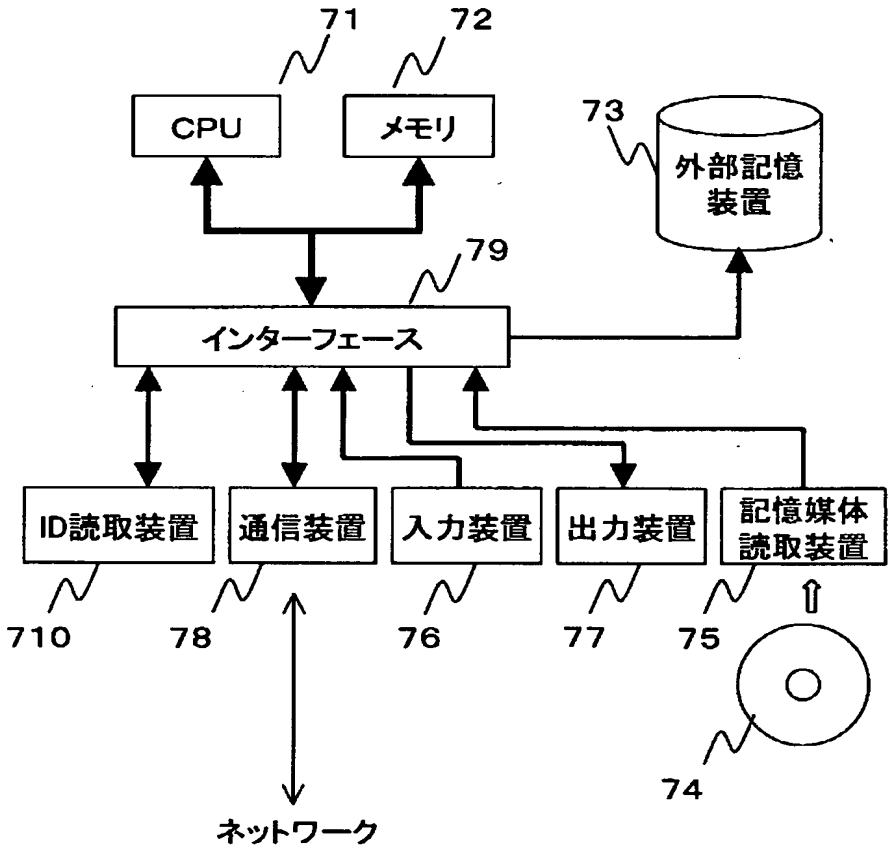
【図７】

図7


ネットワーク2
65
通信部
ID利用端末6
64
データベース
63
制御部
61
読取部
300
IDタグ
拡張ID
62
入出力部

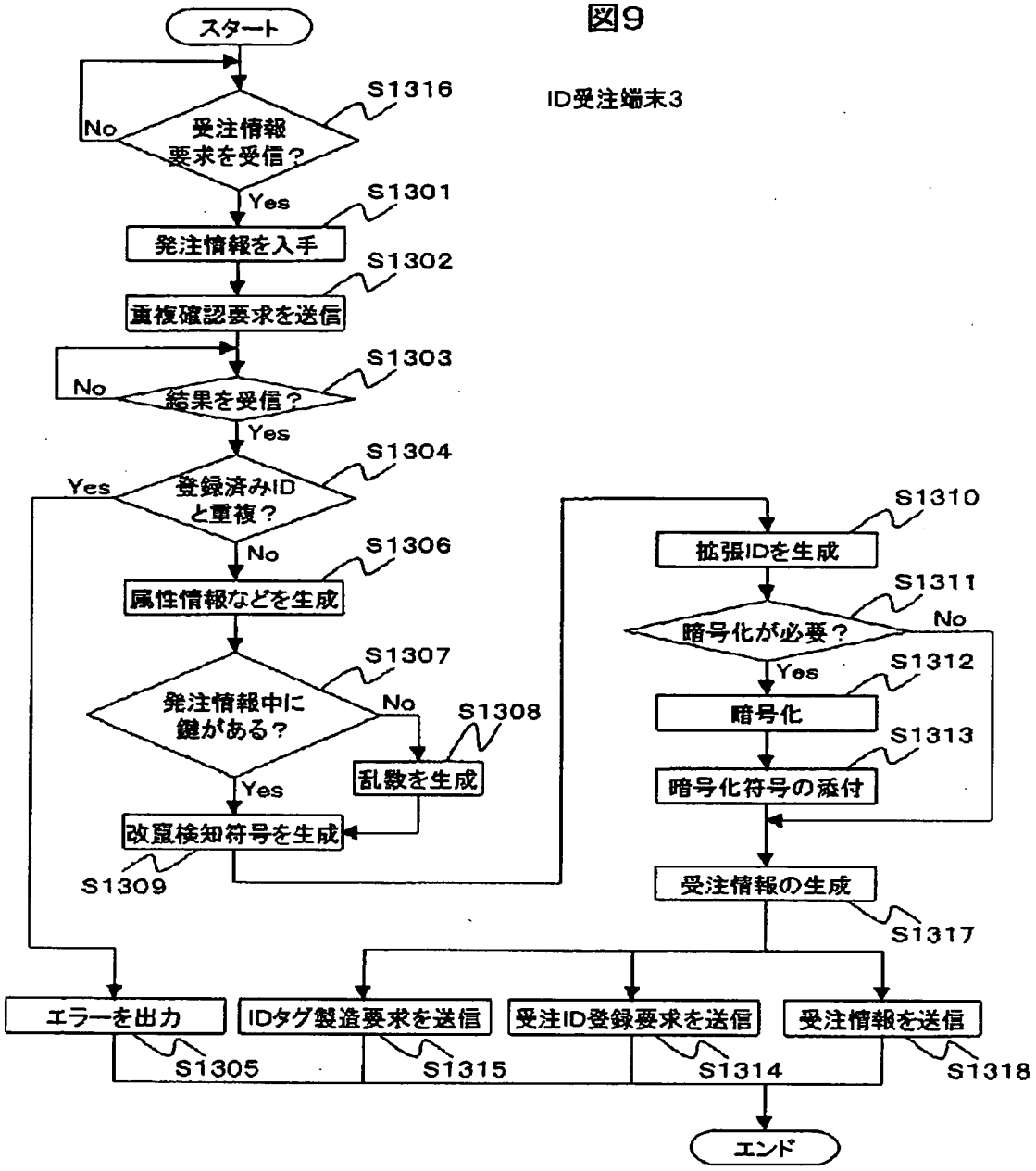
【図８】

図8


71
72
CPU
メモリ
73
外部記憶装置
79
インターフェース
ID読取装置
通信装置
入力装置
出力装置
記憶媒体読取装置
710
78
76
77
75
74
ネットワーク

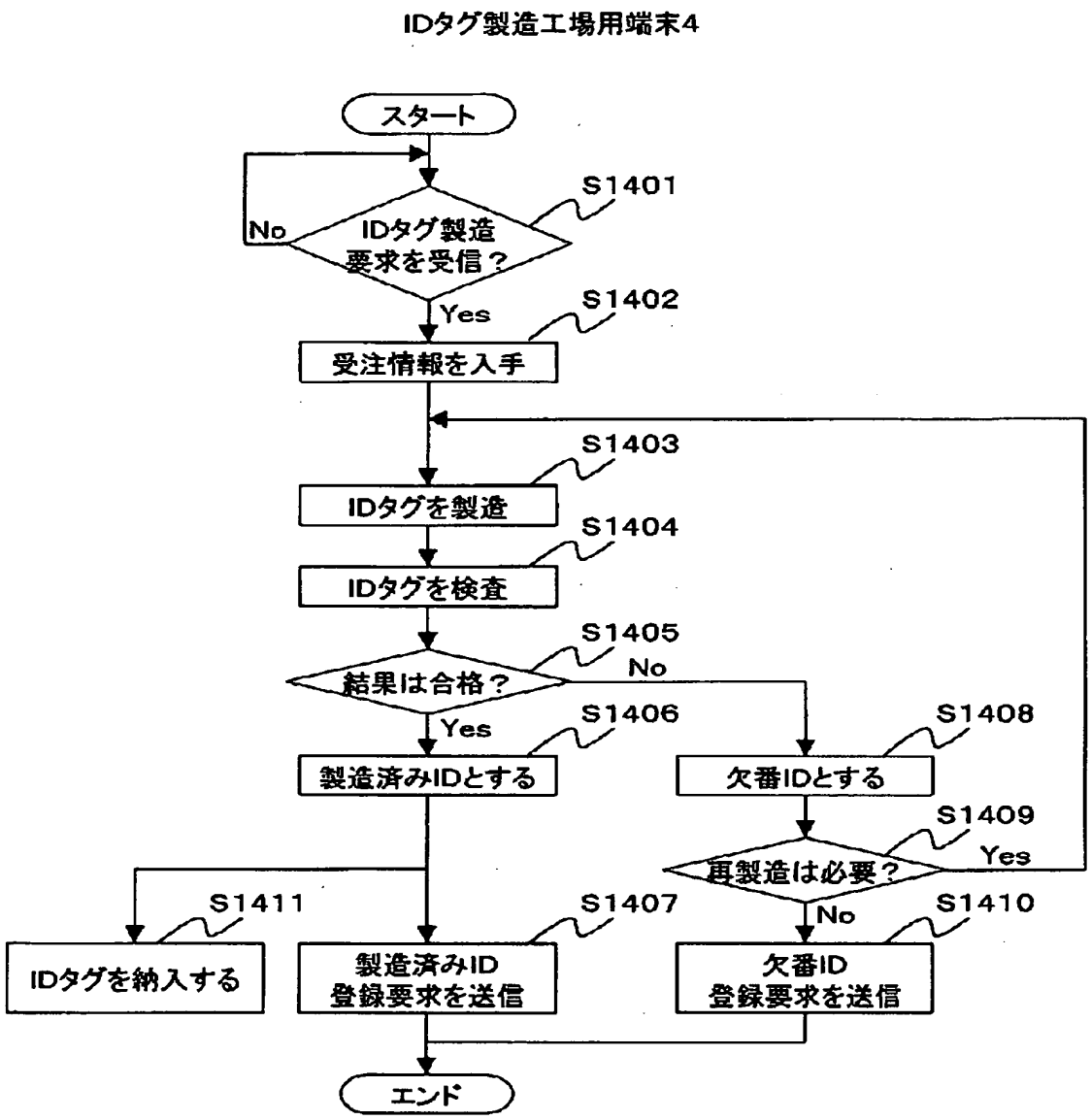
【図９】

図9


ID受注端末3
スタート
S1316
No
受注情報要求を受信？
Yes
S1301
発注情報を入手
S1302
重複確認要求を送信
S1303
No
結果を受信？
Yes
S1304
Yes
登録済みIDと重複？
No
S1306
属性情報などを生成
S1307
発注情報中に鍵がある？
No
S1308
乱数を生成
Yes
改竄検知符号を生成
S1309
S1310
拡張IDを生成
S1311
暗号化が必要？
No
Yes
S1312
暗号化
S1313
暗号化符号の添付
受注情報の生成
S1317
エラーを出力
S1305
IDタグ製造要求を送信
S1315
受注ID登録要求を送信
S1314
受注情報を送信
S1318
エンド

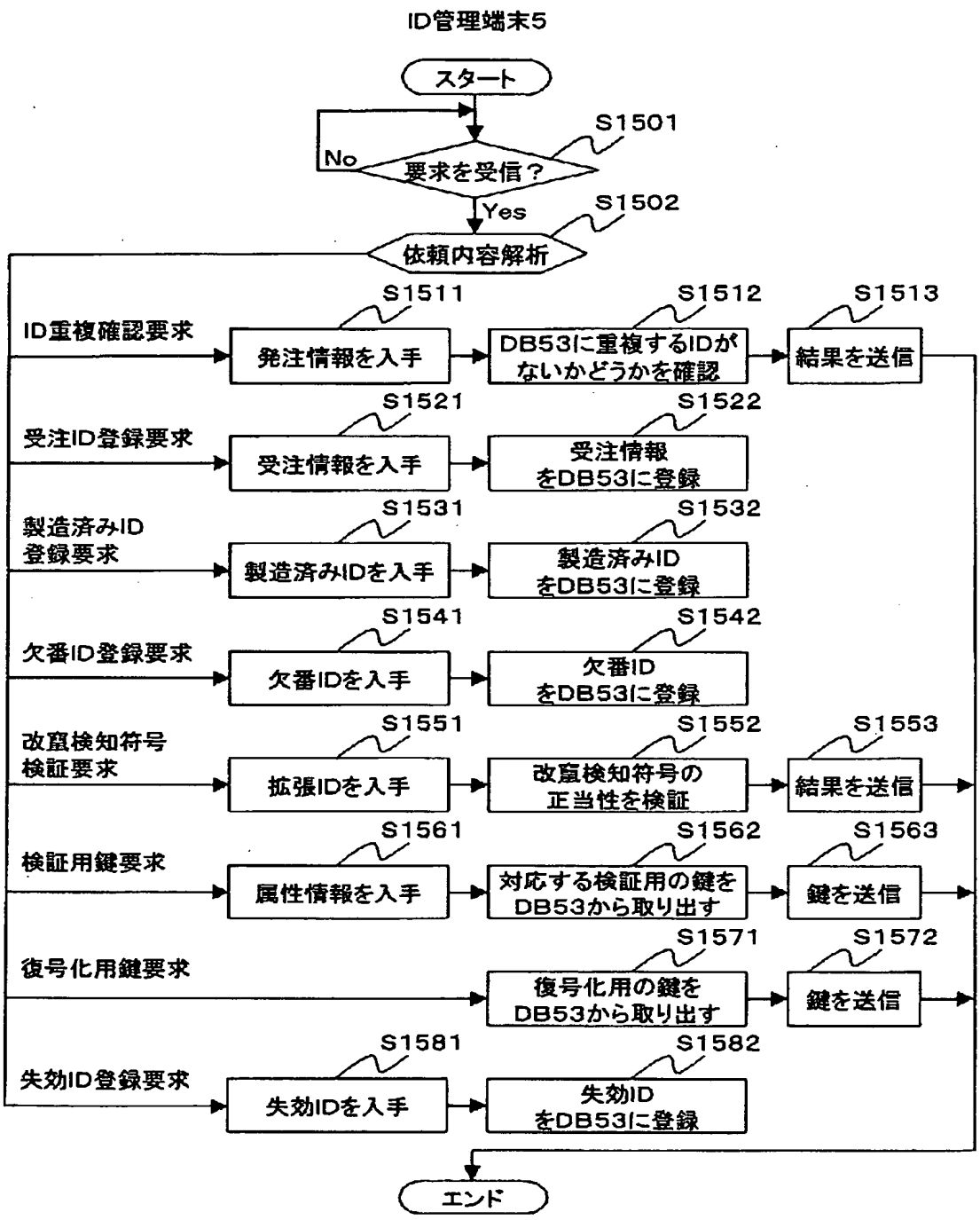
【図１０】

図10


IDタグ製造工場用端末4
スタート
S1401
No
IDタグ製造
要求を受信？
Yes
S1402
受注情報を入手
S1403
IDタグを製造
S1404
IDタグを検査
S1405
結果は合格？
No
Yes
S1406
製造済みIDとする
S1408
欠番IDとする
S1409
再製造は必要？
Yes
No
S1411
IDタグを納入する
S1407
製造済みID
登録要求を送信
S1410
欠番ID
登録要求を送信
エンド

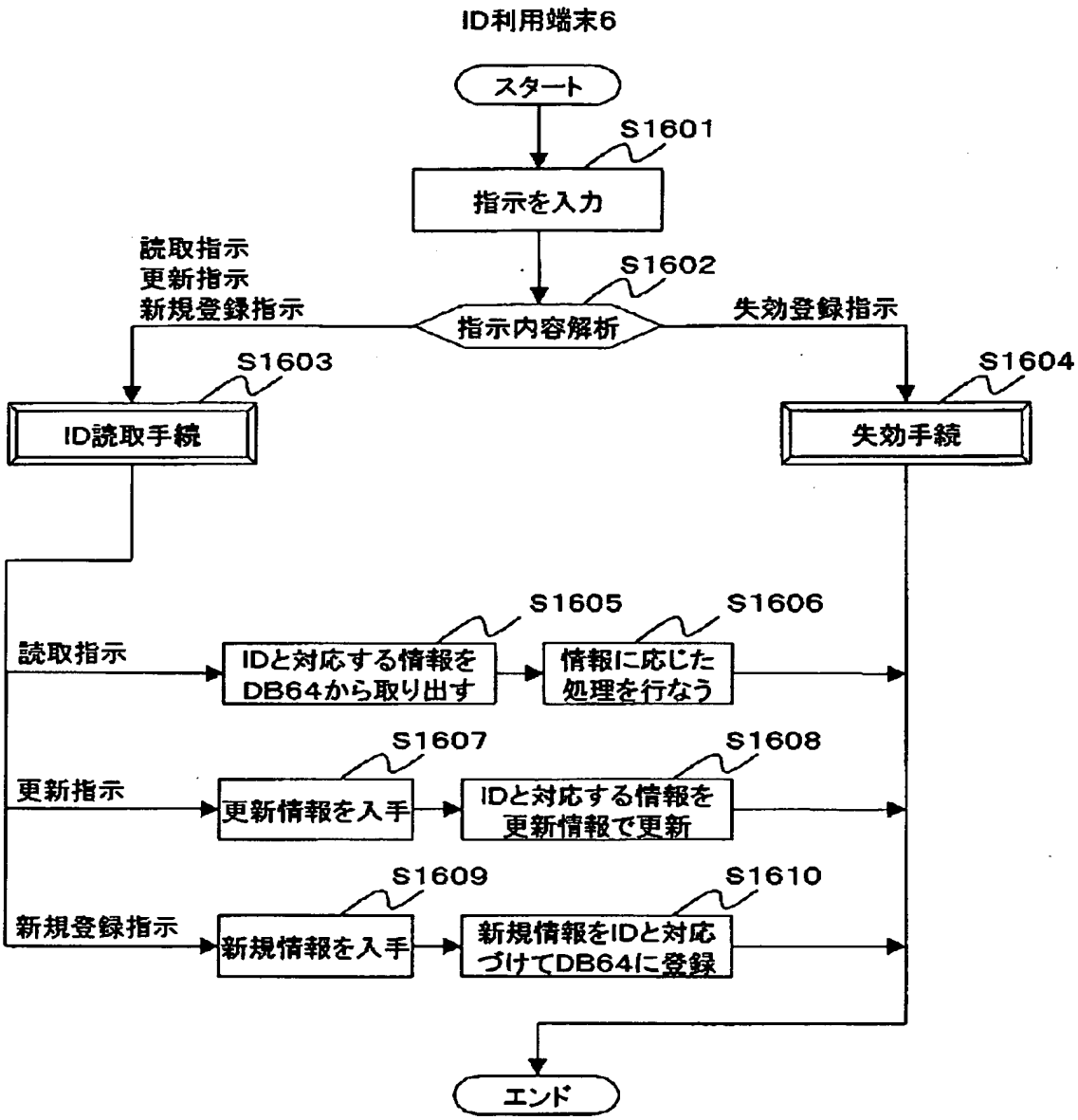
【図１１】

図11


ID管理端末5
スタート
S1501
No
要求を受信？
Yes
S1502
依頼内容解析
ID重複確認要求
S1511
発注情報を入手
S1512
DB53に重複するIDがないかどうかを確認
S1513
結果を送信
受注ID登録要求
S1521
受注情報を入手
S1522
受注情報をDB53に登録
製造済みID登録要求
S1531
製造済みIDを入手
S1532
製造済みIDをDB53に登録
欠番ID登録要求
S1541
欠番IDを入手
S1542
欠番IDをDB53に登録
改竄検知符号検証要求
S1551
拡張IDを入手
S1552
改竄検知符号の正当性を検証
S1553
結果を送信
検証用鍵要求
S1561
属性情報を入手
S1562
対応する検証用の鍵をDB53から取り出す
S1563
鍵を送信
復号化用鍵要求
S1571
復号化用の鍵をDB53から取り出す
S1572
鍵を送信
失効ID登録要求
S1581
失効IDを入手
S1582
失効IDをDB53に登録
エンド

【図１２】

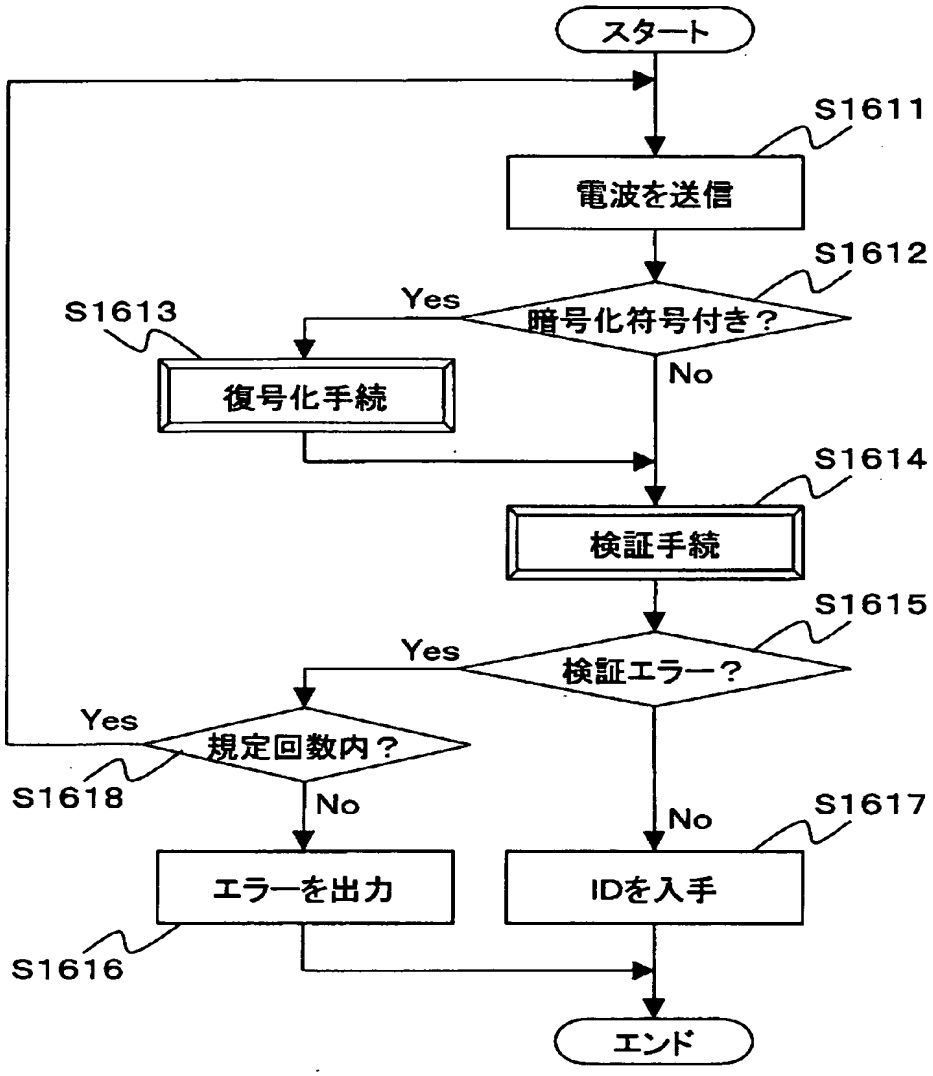
図12


ID利用端末6
スタート
S1601
指示を入力
読取指示
更新指示
新規登録指示
S1602
指示内容解析
失効登録指示
S1603
ID読取手続
S1604
失効手続
S1605
S1606
読取指示
IDと対応する情報をDB64から取り出す
情報に応じた処理を行なう
S1607
S1608
更新指示
更新情報を入手
IDと対応する情報を更新情報で更新
S1609
S1610
新規登録指示
新規情報を入手
新規情報をIDと対応づけてDB64に登録
エンド

【図１３】

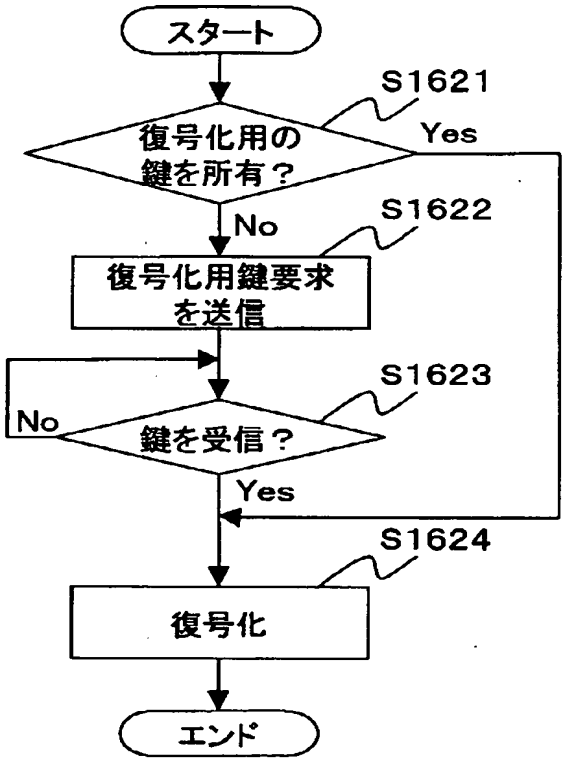
図13

ID読取手続S1603



【図１４】

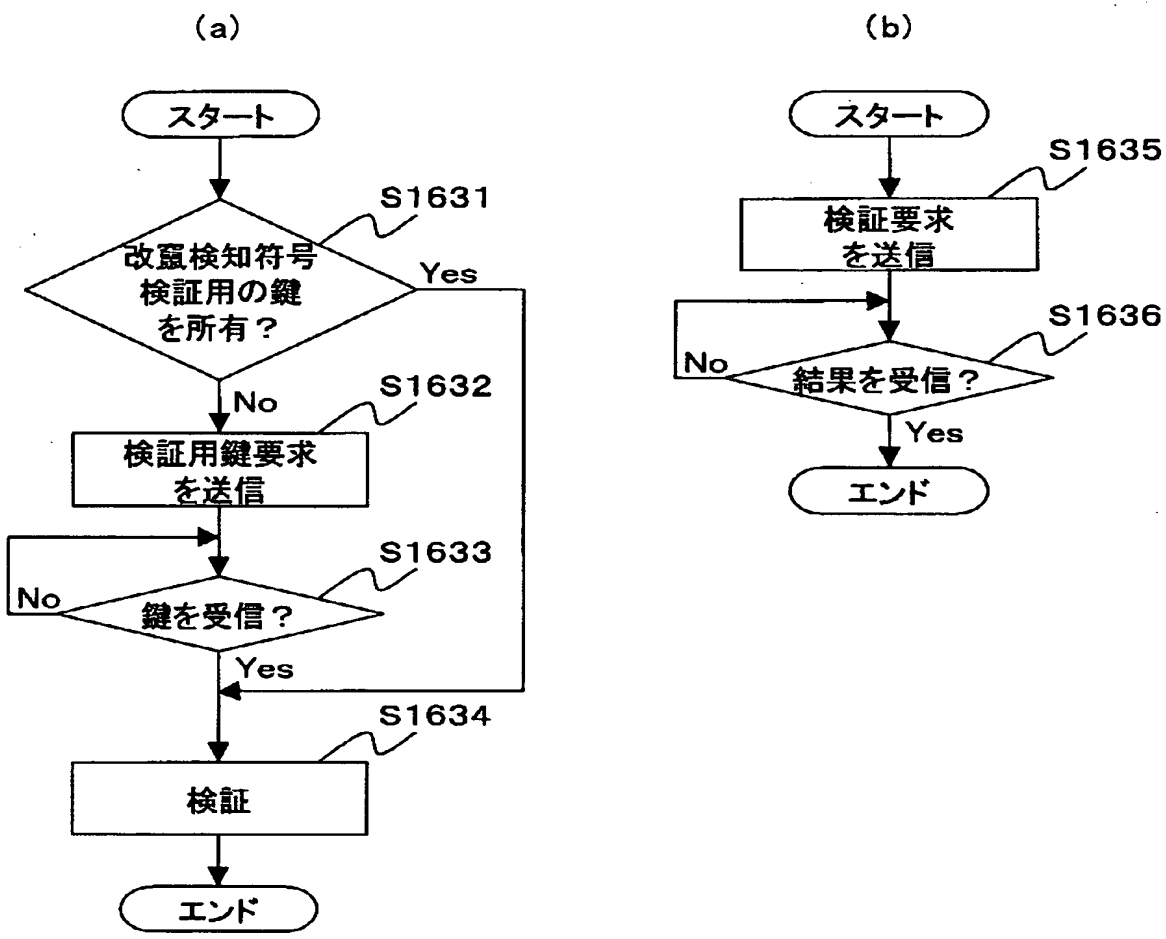
図14


復号化手続S1613
スタート
S1621
復号化用の
鍵を所有？
Yes
No
S1622
復号化用鍵要求
を送信
S1623
No
鍵を受信？
Yes
S1624
復号化
エンド

【図１５】

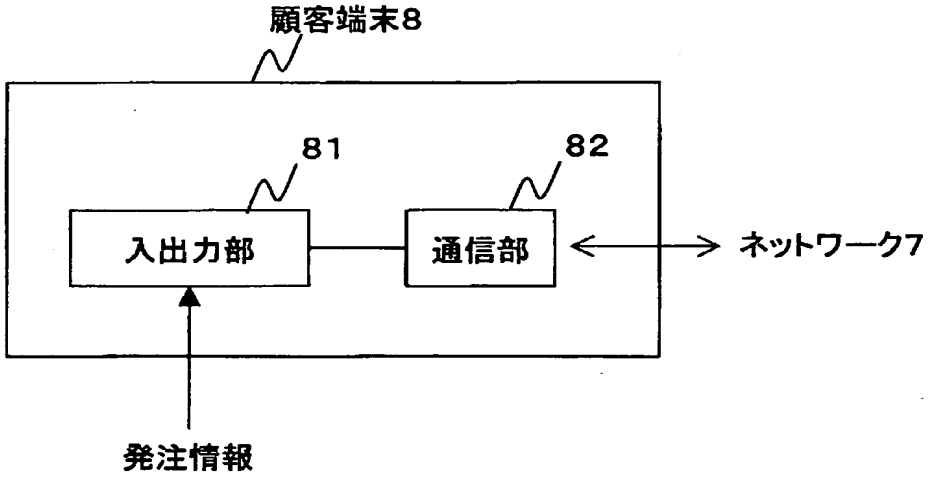
図15

検証手続S1614



【図１６】

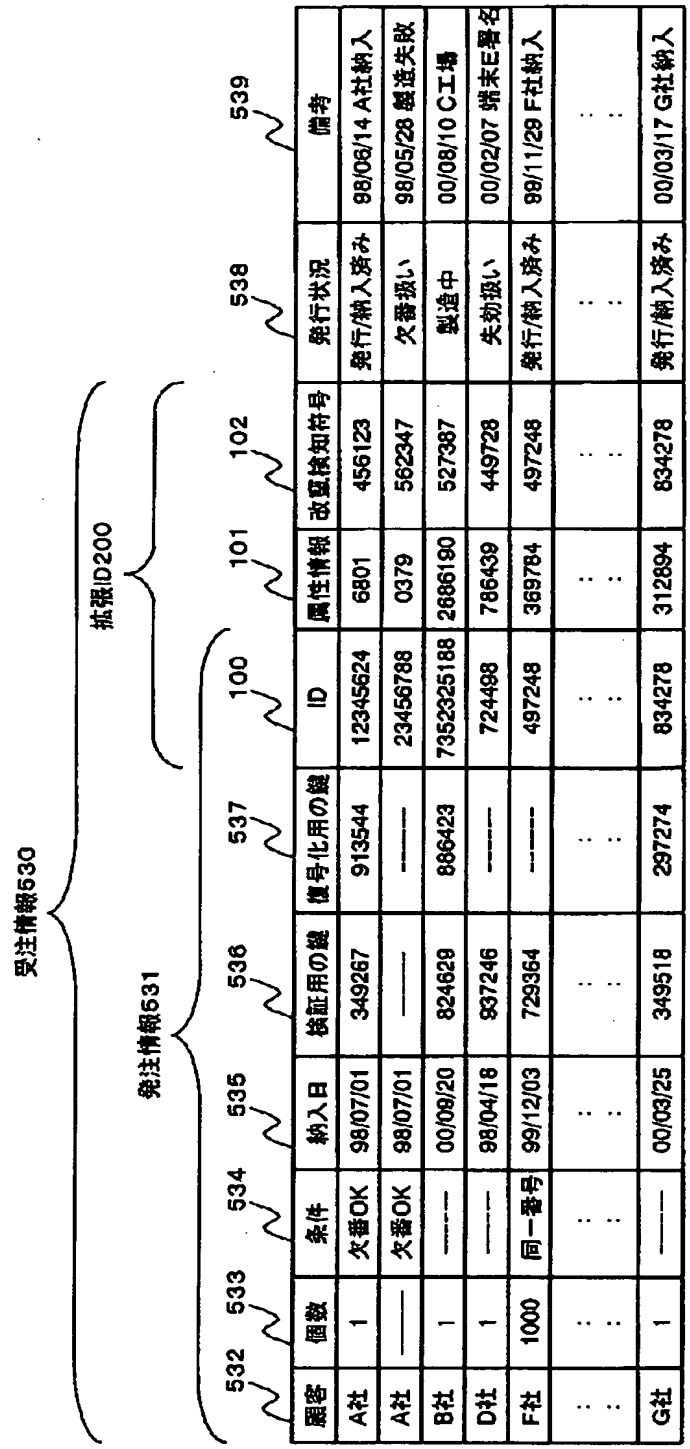
図16



【図１７】

図17

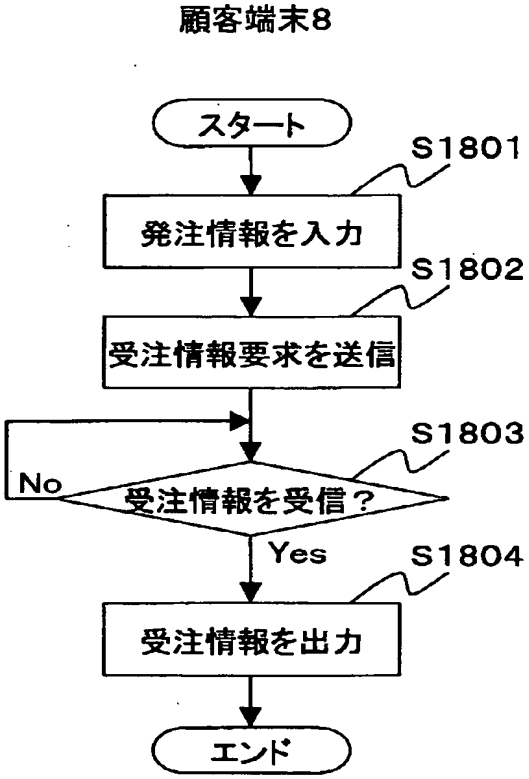
ID関連情報管理データベース53



顧客	個数	条件	納入日	検証用の鍵	復号化用の鍵	ID	属性情報	改竄検知符号	発行状況	備考
A社	1	欠番OK	98/07/01	349267	913544	12345624	6801	456123	発行/納入済み	98/06/14 A社納入
A社	——	欠番OK	98/07/01	——	——	23456788	0379	562347	欠番扱い	98/05/28 製造失敗
B社	1	——	00/09/20	824629	886423	7352325188	2686190	527387	製造中	00/08/10 C工場
D社	1	——	98/04/18	937246	——	724498	786439	449728	失効扱い	00/02/07 端末E署名
F社	1000	同一番号	99/12/03	729364	——	497248	369784	497248	発行/納入済み	99/11/29 F社納入
：：	：：	：：	：：	：：	：：	：：	：：	：：	：：	：：
G社	1	——	00/03/25	349518	297274	834278	312894	834278	発行/納入済み	00/03/17 G社納入

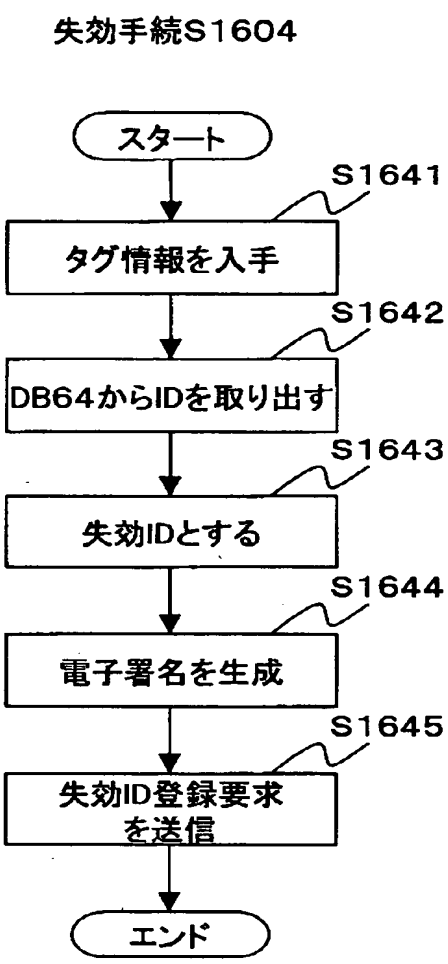
【図１８】

図18


顧客端末8
スタート
S1801
発注情報を入力
S1802
受注情報要求を送信
S1803
No
受注情報を受信？
Yes
S1804
受注情報を出力
エンド

【図１９】

図19


失効手続S1604
スタート
S1641
タグ情報を入手
S1642
DB64からIDを取り出す
S1643
失効IDとする
S1644
電子署名を生成
S1645
失効ID登録要求
を送信
エンド

【書類名】　要約書

【要約】

【課題】

改竄検知符号を備えたIDの発行と流通を管理し、IDを利用した物品管理を効率よく、かつ、信頼性高く行うことが可能な仕組みを提供する。

【解決手段】

改竄検知符号を備えたIDを書き換え不可領域に格納した電子回路チップをIDタグとして用いる。ID受注端末とIDタグ製造工場用端末の情報をID管理端末に集約し、一括管理する。ID利用端末に機密性の高い情報を格納しておかなくてもいいように、前記情報をID管理端末に問い合わせる、または、前記情報の必要な処理をID管理端末に依頼する手段を構築する。

【選択図】　図３

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所